

João Pedro Fachana Cardoso Moreira da Costa

A responsabilidade civil pelos conteúdos ilícitos colocados e difundidos na Internet
Em especial da responsabilidade pelos conteúdos gerados por utilizadores

Dissertação de Mestrado em Direito, na área de
especialização em Ciências Jurídico – Privatísticas,
realizada sob a orientação do Exmo. Senhor Professor
Doutor Manuel A. Carneiro da Frada

Julho de 2011

Aos meus pais

*Logo que, numa inovação, nos mostram
alguma coisa de antigo, ficamos sossegados.*

Friedrich Nietzsche

RESUMO

Esta dissertação tem como objectivo a aplicação do sistema dogmático comum da responsabilidade civil à realidade da Internet, no sentido de determinar de que forma pode o instituto da responsabilidade civil actuar sobre os conteúdos ilícitos colocados e difundidos em rede, em particular quando estes são gerados pelos próprios utilizadores dos serviços da Internet.

Visa-se, em primeiro lugar, explorar questões-chave relativamente à responsabilidade civil do utilizador que coloca ou difunde o conteúdo ilícito em rede, nomeadamente quanto ao preenchimento dos cinco pressupostos da responsabilidade civil, bem como outras questões acessórias como as hipóteses da relevância da culpa do lesado na Internet, bem como o problema que o anonimato na rede levanta.

Num segundo momento, pretende-se explorar a responsabilidade civil dos prestadores de serviços intermediários, cujas actividades são aptas a difundir conteúdos ilícitos na rede. Em particular, estuda-se o regime português vigente relativamente a esta matéria, sem descurar uma análise ao Direito Comparado, nomeadamente o regime comunitário uniforme e o regime norte-americano.

Por fim, pretende-se averiguar se, à luz do paradigma da *web 2.0*, o sistema vigente mantém a sua força original, face às novas tendências que se verificam em vários ordenamentos jurídicos.

Conclui-se pela manutenção, no essencial, do regime de isenção de responsabilidade dos prestadores de serviços intermediários, não obstante a nova realidade da *web 2.0* implicar, pelo menos, uma inversão do ónus da prova das condições de isenção.

ABSTRACT

The objective of this dissertation is the application of the civil liability traditional dogmatic system to the present Internet space, in order to appraise the way that the civil liability approach can be used to act upon unlawful contents uploaded and disseminated in the network, mainly when these are generated by the actual users of Internet-based services.

In a first stage we will focus on key questions concerning civil liability of the user that uploads or disseminates unlawful contents in the network, in particular regarding the fulfillment of the five requirements of civil liability, as well as other issues as the hypothesis of the relevance of guilt of the offended part in Internet context, as well as the problem drawn by anonymity in the network.

In a second moment we will explore civil liability concerning intermediary services providers whose activities are capable of distributing unlawful contents in the network. In particular, we will study the Portuguese legal system concerning this issue without overlooking a comparative law analysis, mainly related to the uniform European legal system and the North American legal system.

Ultimately, we aim to investigate if, under the paradigm of web 2.0, the current system keeps its original strength, when facing the new tendencies that are emerging in several law orders.

We conclude for the maintenance of the core of the regime of exemption of liability for intermediary service providers notwithstanding, at least, that the new web 2.0 reality will require an inversion of the burden of proof of liability exemption.

Agradecimentos

- Aos meus pais, por todo o apoio que me deram, sobretudo nos momentos mais críticos, e pela inestimável ajuda na formatação e correcção bibliográfica da dissertação;

- À minha irmã, pelo companheirismo que sempre demonstrou;

- À JPAB – José Pedro Aguiar–Branco & Associados, na pessoa do meu patrono e colega, Dr. Pedro Botelho Gomes, pelo tempo concedido para a pesquisa bibliográfica e elaboração da dissertação. Um agradecimento especial às minhas colegas, Dra. Joana Carneiro e Dra. Ana Isabel Fidalgo, pela paciência na revisão do texto e pelas úteis sugestões que me deram ao longo deste ano;

- À Senhora Professora Doutora Luísa Neto, por todos os conselhos e exemplos que me transmitiu (e ainda transmite) ao longo do meu percurso académico nesta Faculdade e que, de uma forma ou de outra, influenciaram a presente dissertação;

- Ao Senhor Professor Doutor Sinde Monteiro, que me acompanhou e auxiliou nos primeiros passos desta investigação, encetados durante o *Praticum* em Direito Civil;

- Ao Senhor Professor Doutor Manuel Carneiro da Frada, por ter aceitado orientar a presente tese, bem como por todos os conselhos e ensinamentos oportunos que me transmitiu durante a elaboração da mesma;

Por fim,

- À Xana, pelo precioso apoio e motivação a toda a hora e, acima de tudo, pela paciência e compreensão nas alturas em que não estive tão disponível como desejava.

SUMÁRIO

Capítulo I – A Internet e o Direito

- 1. A Internet e os seus conteúdos 19**
- 2. Os intervenientes na colocação e difusão de conteúdos na Internet 30**

Capítulo II – Pontos críticos na determinação da responsabilidade civil do utilizador que coloca e difunde conteúdos ilícitos na Internet

- 3. Ponto prévio: breve referência à dogmática comum da responsabilidade civil ... 37**
- 4. A ilicitude dos conteúdos colocados e difundidos na Internet..... 39**
- 5. A determinação da culpa do agente na colocação e difusão de conteúdos..... 50**
- 6. O dano 57**
- 7. O nexo de causalidade entre o dano e o facto ilícito: em especial, a potenciação do dano e a sua imputação ao(s) agente(s) 62**
- 8. A exclusão da responsabilidade civil na Internet 64**
- 9. O problema do anonimato na Internet..... 66**

Capítulo III – A responsabilidade civil dos prestadores de serviços intermediários na rede

- 10. Evolução histórica da responsabilização dos prestadores de serviços intermediários..... 71**

11. O panorama vigente: o Regime Jurídico do Comércio Electrónico	80
12. Enquadramento dogmático da responsabilidade civil dos intermediários	90
13. Análise crítica da solução legal acolhida	95
14. Breves considerações sobre os contratos de prestação intermediária de serviços na Internet, em particular na <i>web 2.0</i> , e a sua aplicabilidade relativamente a conteúdos ilícitos colocados e difundidos em rede.....	106
15. Balanço do sistema acolhido: a primazia da eficiência do comércio electrónico sobre a tutela efectiva do lesado.....	113
 Capítulo IV – As novas tendências face ao regime vigente, no arquétipo da <i>web 2.0</i>.	
16. A exclusão do regime de isenção de responsabilidade com base na ausência da neutralidade típica da actividade de intermediação de serviços <i>online</i>	115
17. A obrigação de monitorização <i>a priori</i> de conteúdos. A colocação de filtros.....	120
18. Reincidências sobre a responsabilidade do dono da coisa. O exemplo paradigmático da Lei HADOPI	129
19. O Tratado ACTA.....	135
20. Caminhos a trilhar?	138
 Conclusões.....	 145

ABREVIATURAS

CC – Código Civil

CDADC – Código de Direitos de Autor e Direitos Conexos

CPI – Código da Propriedade Industrial

DCE – Directiva sobre o Comércio Electrónico

DMCA – *Digital Millenium Copyright Act*

DPI – *Deep Packet Inspection*

IP – *Internet Protocol*

P2P – *Peer-to-peer*

RJCE – Regime Jurídico do Comércio Electrónico

TCP – *Transmission Control Protocol*

TCP/IP – *Transmission Control Protocol / Internet Protocol*

INTRODUÇÃO

A dissertação que aqui se apresenta visa abordar a problemática da responsabilidade civil pelos conteúdos ilícitos colocados e difundidos na Internet, em particular quando tais conteúdos são gerados pelos próprios utilizadores dos serviços da Sociedade da Informação.

Na primeira década do presente milénio assistiu-se a uma evolução da Internet e da *world wide web* (www) a todos os níveis, sendo que a face mais visível dessa evolução se traduziu, e traduz no presente, pela proliferação de serviços tendencialmente gratuitos que permitem aos utilizadores desses mesmos serviços a colocação e transmissão de conteúdos por eles próprios gerados – é o advento da chamada *web 2.0*. O utilizador da Internet deixou de ser mero consumidor de serviços disponibilizados em linha, para ser, ele próprio, activo participante na criação e desenvolvimento desses mesmos serviços.

Como contraponto deste desenvolvimento espantoso da *www* constatou-se, igualmente, um proliferar de situações e actos ilegais, que provocam danos em terceiros, *maxime* através da colocação e difusão em rede de conteúdos ilícitos. Assim, o estudo da aplicação da responsabilidade civil à realidade fáctica – e também jurídica – da Internet e, em particular, da *web 2.0*, assume particular pertinência.

Pretende-se, pois, com a presente dissertação, aplicar o sistema dogmático comum da responsabilidade civil a esta nova realidade, enunciando os principais problemas que a efectivação prática da mesma pode suscitar no mundo digital. Deste modo, porque existe a consciência que nos iremos debruçar sobre um tema pouco conhecido (e estudado) no universo jurídico português, esta tese assume explicitamente um cariz expositivo, não obstante a tomada de posições críticas quando as mesmas se reputem por necessárias.

No Capítulo I desta dissertação começaremos por contextualizar o leitor no mundo digital que consubstancia a Internet. Efectuaremos, pois, uma breve súmula da evolução histórica da Internet desde os primórdios da sua criação até ao panorama vigente da *web 2.0*. Identificaremos também os principais intervenientes na colocação e difusão de conteúdos na Internet, entre os quais se encontram os utilizadores da mesma e os prestadores de serviços intermediários em rede.

Assim, no capítulo II iremos analisar as principais questões que se podem colocar no âmbito da determinação da responsabilidade civil dos utilizadores dos serviços da Internet, autores da colocação e eventual difusão dos conteúdos ilícitos em rede. Não deixaremos, porém, de analisar, também, em que medida uma eventual culpa do lesado na produção do efeito danoso poderá ser valorada na realidade da Internet. Por fim, analisaremos o grande problema que obsta à eficácia da responsabilidade civil dos autores do acto ilícito: o anonimato na rede.

Atendendo ao obstáculo evidenciado, no capítulo III analisaremos em que moldes se poderá, eventualmente, responsabilizar civilmente o prestador do serviço intermediário em rede através do qual o conteúdo ilícito foi colocado e/ou difundido. Faremos uma breve súmula de Direito Comparado sobre as concepções dogmáticas dos ordenamentos jurídicos que mais se têm debruçado sobre esta matéria, bem como sobre o “estado da arte” no dealbar do novo milénio.

Ainda a respeito da responsabilidade civil dos prestadores de serviços intermediários em rede, analisaremos criticamente o regime jurídico vigente em Portugal, dado pelo Decreto-Lei n.º 7/2004 de 7 de Janeiro, alterado pelo Decreto-Lei n.º 62/2009 de 10 de Março, que transpôs para o ordenamento jurídico nacional a Directiva n.º 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de Junho de 2000, apontando eventuais caminhos doutrinários a seguir na delimitação de alguns dos seus conceitos, bem como procedendo a um enquadramento dogmático da responsabilidade civil dos intermediários. Procuraremos ainda não descurar a análise hipotética da existência de responsabilidade civil dos prestadores de serviços intermediários por conteúdos ilícitos colocados em rede por terceiros em face dos deveres de protecção que eventualmente surjam em contratos de prestação de serviços da *web 2.0* celebrados entre aqueles e os utilizadores lesados ou, até, a hipotética possibilidade de extensão desses deveres a terceiros lesados, não partes no contrato.

Por fim, no último capítulo desta dissertação, analisaremos algumas novas tendências jurisprudenciais e legislativas que têm ocorrido em diversos ordenamentos jurídicos, com vista a avaliar a razoabilidade da manutenção do actual regime vigente da responsabilidade civil por conteúdos ilícitos colocados e difundidos na Internet face ao paradigma actual da *web 2.0*. Concluiremos, pois, apontando caminhos para uma eventual mudança do regime

vigente, atendendo aos novos desenvolvimentos das tecnologias de informação, *maxime*, da Sociedade da Informação.

CAPÍTULO I

A INTERNET E O DIREITO

1. A Internet e os seus conteúdos

1.1. Ponto Prévio: Da noção de conteúdo colocado e difundido na Internet

A palavra “conteúdo”, no dicionário *online* da língua portuguesa *Infopédia*¹, é apresentada como “aquilo de que algo é constituído”. É, assim, uma palavra que surge necessariamente ligada a outra.

Para o estudo que nos propomos fazer, urge necessariamente definir o que é um conteúdo colocado e difundido na Internet. Neste contexto, o conteúdo será sempre uma informação digital: uma informação que reproduz texto, imagem, som, ou multimédia², que é colocada na Internet e difundida através de dispositivos de *hardware* e *software* próprios daquela.

De modo semelhante definiu o Ministério da Ciência e da Tecnologia, em 1997, a palavra conteúdo, referindo, no seu Livro Verde para a Sociedade da Informação, que “no contexto emergente da Sociedade da Informação, o termo “conteúdo” parece englobar todo e qualquer segmento de informação propriamente dito, isto é, tudo aquilo que fica quando excluímos os sistemas de *hardware* e *software* que permitem a sua consulta e exploração”³.

Assim, será esta definição de conteúdo a que nos estaremos a referir, sempre que utilizarmos a expressão ao longo do presente estudo.

1.2. Da criação da Internet à web 2.0.

Como muitas das tecnologias de informação existentes, a Internet não foi inicialmente criada para servir e ser utilizada pela população em geral⁴. No ano de 1958, em pleno clima de

¹ Vide www.infopedia.pt (consult. em 27.07.2011).

² Neste caso, conjugando duas ou mais vertentes das referidas anteriormente.

³ Apud SOFIA DE VASCONCELOS CASIMIRO, *A Responsabilidade Civil pelo conteúdo da Informação transmitida pela Internet*, p. 15.

⁴ Seguimos, de perto, a evolução histórica da Internet indicada por GARCIA MARQUES e LOURENÇO MARTINS, *Direito da Informática*, p. 56 ss.

Guerra-fria⁵, foi criada a DARPA (*Defence Advanced Research Projects Agency*) pelos Estados Unidos da América. Esta agência foi criada com o intuito de coordenar projectos de investigação para o Departamento de Defesa dos EUA. Em 1969, a DARPA inaugurou uma rede de comunicações para organizações ligadas à investigação científica na área da Defesa, à qual chamou ARPANET (*Advanced Research Projects Agency Network*). A tecnologia da ARPANET consistia numa rede sem qualquer servidor central, responsável pelo correcto funcionamento dos vários servidores existentes em cada ponto de comunicação. Tal fora assim concebido para impedir que, caso um servidor fosse atacado, a rede deixasse de funcionar. Com este sistema, onde todos os pontos se equivaliam, a destruição ou mau funcionamento de um não se alastraria aos demais e, por conseguinte, a ARPANET manter-se-ia em funcionamento.

Cedo, a tecnologia idealizada com a ARPANET passou a ser usada noutros sectores, como Universidades ou grandes organizações. Assim, durante a década de oitenta do séc. XX, surgiu a denominação Internet (*Interconnected Networks*). A Internet começou a ser usada em Universidades e grandes empresas nos EUA e, depois, noutros países. Consistia numa *rede de redes*, isto é, uma interconexão de redes diferentes entre si, mas que permaneciam ligadas e comunicavam através de um protocolo denominado TCP/IP (*Transmission Control Protocol / Internet Protocol*)⁶. A Internet, ao contrário da sua antecessora, a ARPANET, encontra-se concebida para os utilizadores comuns, funcionando com uma dupla finalidade: publicação e comunicação de informações ou conteúdos.

A Internet, antes da década de 1990, ainda não tinha o carácter internacional que hoje apresenta. Existiam várias Internetes, cada qual com o seu fim específico (militar, universitário, empresarial, ou outro), mas ainda não existia a interconexão entre todas essas redes. De todo o modo, na origem da Internet sempre esteve o desígnio de que esta não servisse apenas uma finalidade singular, mas sim uma finalidade geral, dotada de uma estrutura onde novas aplicações pudessem ser concebidas e desenvolvidas, o que veio a suceder com a criação da *World Wide Web* (www)⁷.

⁵ Relembre-se que, no ano de 1957, a U.R.S.S. tinha dado um passo em frente em relação aos EUA, ao lançar o satélite *Sputnik* e dando, assim, início à corrida pela conquista do espaço.

⁶ O TCP é um mecanismo de transporte, orientado para a conexão de dados e que fornece uma ligação confiável, garantindo assim que os dados cheguem íntegros ao local de destino. Por sua vez, o IP executa a tarefa básica de levar pacotes de dados da origem para o destino. O protocolo IP serve também de identificação do computador que emite os dados para serem transportados na rede, o que, como veremos *infra*, pode ser importante para a identificação dos utilizadores que colocam e difundem conteúdos na Internet.

⁷ Vulgarmente traduzida como “teia do tamanho do mundo”. Vide GARCIA MARQUES e LOURENÇO MARTINS, *op. cit.*, p. 59.

A filosofia subjacente à Internet e à sua consistência tecnológica era imanente à sua natural evolução e expansão. Com o acesso livre à Internet, em especial aos protocolos que compunham a sua estrutura (como o já referido protocolo TCP/IP), esta cresceu rapidamente.

No entanto, a verdadeira democratização da Internet chegou no início da década de 1990, com a criação da já referida *World Wide Web*. A *www* foi criada por uma equipa coordenada por Tim Berners-Lee e Robert Cailliau, cujo intento originário era a fácil partilha de documentos científicos. Com a *www* qualquer pessoa, desde que possuísse um computador com ligação à Internet (nomeadamente através da utilização de um *modem*), podia navegar livremente na rede e procurar aceder a informação, em qualquer lugar do globo.

A *www* consiste, deste modo, numa área da Internet onde se colocam diversos blocos de informação com texto, gráficos, elementos multimédia, como som ou vídeo, encontrando-se os diversos blocos interligados por *hyperlinks*⁸. A sua simples interface levou a que se expandisse espectacularmente nessa década, tornando-se assim o mais importante componente da Internet, enquanto meio de comunicação e interacção entre as pessoas, bem como de transmissão de informação a nível global, rápida e sem barreiras⁹.

Todavia, a *www*, apesar de ter tornado a Internet acessível a todos, requeria ainda um elevado conhecimento de informática para que um utilizador não especialista conseguisse criar o que se convencionou designar por “uma página *web*” e alojá-la num determinado servidor. Assim, até ao início do século XXI, a utilização corrente da Internet era meramente passiva, isto é, de consulta e obtenção de informação ou de conteúdos. Excepcionava-se o envio de informações e ou documentos por via do correio electrónico ou a transmissão de informações através do *Internet Relay Chat (IRC)*¹⁰.

A implementação da *www*, para além de proporcionar o crescimento exponencial do uso da Internet, levou igualmente à expansão do comércio electrónico¹¹. Como aponta ALEXANDRE DIAS PEREIRA, se até à década de 1990, o comércio electrónico existia

⁸ O *hyperlink*, designado em português por hiperligação, é um processo de comunicação entre blocos diversos de informação, seleccionável através de elementos desses mesmos blocos.

⁹ Vide GARCIA MARQUES e LOURENÇO MARTINS, *op. cit.*, p. 60.

¹⁰ O *Internet Relay Chat* “possibilita a comunicação em tempo real entre assinantes da Internet, permitindo organizar reuniões face a face e o intercâmbio de material.” Vide GARCIA MARQUES e LOURENÇO MARTINS, *op. cit.*, p. 59. O *software* mais conhecido de utilização do *IRC* é o *mIRC*.

¹¹ Não existe uma única definição para comércio electrónico. Segundo a ANACOM (Autoridade Nacional de Comunicações), por comércio electrónico entende-se a actividade de “realização de transacções de bens e serviços entre computadores mediados por redes informáticas, sendo que o pagamento e ou a entrega dos produtos transaccionados não são, necessariamente, efectuados por via electrónica.” Vide JOEL RAMOS TIMÓTEO PEREIRA, *Compêndio Jurídico da Sociedade da Informação*, p. 384. Já ALEXANDRE DIAS PEREIRA, *Comércio electrónico na Sociedade da Informação: da segurança técnica à confiança jurídica*, p. 14, refere que o “comércio electrónico traduz-se na negociação realizada por via electrónica, isto é, através do processamento e transmissão electrónicos de dados, incluindo texto, som e imagem.”

apenas entre empresas, realizado através de redes fechadas específicas (como o *Electronic Data Interchange* – EDI), com a *www* o comércio electrónico expandiu-se numa “complexa rede de actividades comerciais efectuadas à escala mundial entre um número cada vez maior de participantes, empresariais e individuais, e em redes abertas como a Internet”¹².

A evolução do comércio electrónico foi tal que a negociação e contratação informática deixou de incidir apenas sobre bens corpóreos, físicos, do mundo real, para passar a incidir também sobre bens incorpóreos, imateriais, do mundo virtual. A Internet deixava, assim, de ser apenas um meio para o comércio, para passar a ser o objecto do comércio em si. Seguindo esta linha de raciocínio, passou a ser possível distinguir duas modalidades de comércio electrónico¹³:

- *Comércio electrónico indirecto*: Trata-se da encomenda electrónica de bens corpóreos, cujo pagamento pode ser feito através da própria Internet, mas a entrega do bem é feita pelos meios tradicionais (p.e. serviços postais);

- *Comércio electrónico directo*: Consiste na encomenda electrónica de bens incorpóreos e serviços, cujo pagamento e entrega é feita através da própria rede da Internet.

Ambas as modalidades de comércio electrónico referidas tiveram uma ampla difusão desde a década de 1990 e até aos nossos dias. Outra das características do comércio electrónico prende-se com o facto de não ser necessariamente uma actividade realizada por comerciantes¹⁴. Na verdade, os utilizadores “normais” da Internet e da *www* cedo começaram a utilizar vários serviços do comércio electrónico, não só para fazerem as suas “compras *online*”, mas também para usufruírem de vários serviços na própria *www*, como a obtenção de uma conta e endereço de e-mail, a subscrição de *sites* com vários conteúdos para *download*, a subscrição de fóruns *online* ou de *bulletin boards*, o “aluguer” de um espaço na rede para a construção de uma *homepage*, entre outros.

Até ao dealbar do novo milénio, a maior parte dos serviços proporcionados na *www* exigia dos utilizadores o pagamento de um determinado valor para que estes pudessem usufruir do serviço. Por outro lado, como já referido, para que um utilizador tivesse um papel mais activo na rede era-lhe exigido um conhecimento informático superior ao do utilizador

¹² Vide ALEXANDRE LIBÓRIO DIAS PEREIRA, *Comércio Electrónico* ..., pp. 14 e 15.

¹³ *Idem*, *Ibidem*.

¹⁴ Vide ALEXANDRE LIBÓRIO DIAS PEREIRA, “Princípios do Comércio Electrónico”, in *Miscelâneas do Instituto de Direito das Empresas e do Trabalho*, n.º 3, p. 78 ss. Este autor refere inclusive que o comércio electrónico não é, nem por lei nem por natureza, uma actividade comercial, o que não significa que muitas das actividades que dão forma ao comércio electrónico não assumam natureza comercial.

comum para criar a sua própria página na Internet. Acresce que os *sites* existentes na *www* apresentavam, na sua generalidade, as seguintes características:

- *Apresentavam conteúdos estáticos* – Isto é, os conteúdos da página nunca mudavam, permanecendo sempre iguais, o que levava a que os utilizadores não se sentissem compelidos a voltar ao *site* após a sua visualização;

- *Não eram interactivos* – Os utilizadores que visitavam o *site* não podiam contribuir para a adição de outros conteúdos ou para a modificação dos conteúdos existentes¹⁵;

- *Eram desenvolvidos tendo em conta uma filosofia fechada* – Ou seja, os códigos informáticos que criavam as aplicações disponibilizadas nos *sites* não eram divulgados, permitindo apenas o acesso ao produto final, o que impedia os utilizadores (ou outros agentes económicos) de utilizar esses códigos para desenvolverem ou aperfeiçoarem as aplicações disponibilizadas nos *sites*.

Este modo de concepção na elaboração das páginas e *sites web* levou a uma quebra na expansão do comércio electrónico. Com efeito, os operadores económicos que actuavam na rede depressa se aperceberam que não se encontravam a utilizar todas as potencialidades que a Internet no geral e a *www* em particular podiam proporcionar. Assim, no início do século XXI, os agentes económicos passaram a investir em serviços que potenciassem a interactividade; no fundo, começou a assistir-se à proliferação de serviços cuja principal força motora era a colaboração e a partilha entre os seus utilizadores. De um sistema fechado, virado para uma utilização passiva da rede, passou-se para um sistema aberto, cuja ideia-base é a utilização activa da rede (ou, melhor dizendo, a utilização *proactiva* da mesma).

A esta nova maneira de ver a utilização da Internet, TIM O'REILLY¹⁶, em 2004, apelidou de *web 2.0*¹⁷, por contraposição à anterior *web 1.0*.

O'REILLY deu a seguinte definição de *web 2.0*¹⁸:

¹⁵ Exceptuavam-se os *bulletin boards* e os *newsgroups*, bem como os *fóruns*, cuja filosofia – a permissão de colocação de mensagens de texto numa plataforma alojada num servidor – apontava o caminho da interactividade.

¹⁶ Tim O'Reilly é o fundador e CEO da empresa *O'Reilly Media, Inc.*, cujo objecto comercial é a publicação de livros de Informática e a organização de Conferências no mesmo tema. O seu *site* pode ser visualizado em <http://oreilly.com> (último acesso em 27.07.2011)

¹⁷ A *web 2.0*, ao contrário do que possa parecer, não configura uma evolução tecnológica da *www* ou da própria Internet em si. Na verdade, os serviços da *web 2.0*, em termos tecnológicos, já eram possíveis desde a altura da criação da *www* – existem antes do século XXI, como são exemplo disso os *bulletin boards*, *newsgroups* e *fóruns*. Embora a existência da *web 2.0* não seja consensual entre a comunidade informática, a verdade é que ela representa uma nova cultura existente na actual comunidade de internautas, onde o centro da atenção recai sobre o utilizador.

¹⁸ *Apud* CARLISLE GEORGE e JACKIE SCERRI, “Web 2.0 and User – Generated Content: Legal challenges in the new frontier”, in *Journal of Information, Law and Technology*, p.3.

“A *web 2.0* é a rede, enquanto plataforma, que engloba todos os dispositivos a ela ligados; as aplicações da *web 2.0* são aquelas que aproveitam o máximo das vantagens intrínsecas àquela plataforma: disponibilizando *software* como um serviço actualizado de forma contínua, que melhora ao ritmo a que cresce o número de pessoas que o utiliza, consumindo e modificando dados de variadas fontes, incluindo de utilizadores individuais, enquanto fornecem os seus próprios dados e serviços numa forma que permite a sua alteração por outros, criando efeitos na rede através de uma “arquitectura de participação” e indo para além da *web 1.0* para trazer experiências ao utilizador mais ricas”¹⁹.

Na essência da *web 2.0* incluem-se os seguintes princípios-base²⁰:

- Uso da rede para distribuição de serviços que aproveitam o poder colectivo dos utilizadores – isto significa que, ao contrário do que sucedia com a *web 1.0*, em que as empresas, para aumentarem a rapidez do seu serviço, tinham de criar mais servidores, a qualidade e rapidez do serviço aumenta à medida que aumenta o número dos respectivos utilizadores²¹;

- Fornecimento de serviços economicamente rentáveis, sem dependerem, em regra, de qualquer tipo de pagamento por parte dos respectivos utilizadores – o que potencia o número de utilizadores do serviço – e cujo financiamento, ao invés, é feito através de anúncios publicitários colocados nas páginas *web* dos serviços a que respeitam;

- Controlo sobre fontes de dados únicas que ficam cada vez mais ricas consoante mais utilizadores as usem – quanto a este aspecto, refira-se que mesmo os serviços da tradicional *web 1.0* passaram a utilizar alguns mecanismos da *web 2.0* de modo a potenciar as vendas de produtos, tais como a inclusão da possibilidade de os utilizadores colocarem comentários sobre os produtos disponíveis para venda ou avaliarem-nos de acordo com uma determinada escala²²;

¹⁹ Tradução livre e itálico nossos.

²⁰ Vide CARLISLE GEORGE e JACKIE SCERRI, *op. cit.*, p. 3.

²¹ O maior exemplo a este respeito são os *softwares* que permitem o download *peer-to-peer* (P2P), que consiste na criação de uma rede entre os computadores dos vários utilizadores, de modo a que uns façam download de conteúdos existentes nos computadores de outros utilizadores. Assim, o computador de cada utilizador deste serviço serve também de servidor de alojamento de conteúdos e, quantos mais utilizadores possuírem um determinado conteúdo alojado no seu sistema (e disponível para partilha em P2P), mais rápido se torna o download desse mesmo conteúdo por outros utilizadores que o desejem. Sobre a tecnologia P2P e os potenciais conflitos com a tutela de direitos de autor vide JOSÉ ALBERTO VIEIRA, “Download de obra protegida pelo Direito de Autor e uso privado”, in *Direito da Sociedade da Informação*, Vol. VIII, p. 421 ss.

²² Refira-se, a título de exemplo, a *Amazon* (www.amazon.com), empresa líder no mercado do comércio electrónico indirecto, que criou a possibilidade de os utilizadores avaliarem e comentarem os produtos disponíveis para venda, vulgarmente designada como *user review*.

- Confiança nos utilizadores enquanto co-criadores dos serviços – através da criação, no serviço prestado, de um sistema aberto que permite aos utilizadores actualizar e inovar permanentemente os conteúdos disponibilizados no serviço²³;

- Aproveitamento da inteligência colectiva – tal sucede em várias áreas do comércio electrónico directo: ou como modo de induzir os utilizadores a comprar produtos mais populares (através do chamado *user review*), ou como modo de aumentar as potencialidades do serviço (como no caso da *Wikipedia*) ou ainda como modo de aumentar a interactividade entre os utilizadores (são disso exemplo as *redes sociais*, os *blogues* e a *blogosfera*, entre outros);

- Modo de utilização do serviço simples e acessível a qualquer tipo de utilizador, independentemente do seu nível de conhecimentos informáticos;

- Uso de *software* que permite a sua acessibilidade por mais do que um meio de comunicação – isto é, os serviços da *web 2.0* são acessíveis não só através de um computador, mas também através de outros dispositivos de telecomunicações, como sejam os telemóveis, *iPods*, *iPads*, etc...²⁴.

Assim, com o advento da *web 2.0* e da filosofia que lhe está subjacente – o fornecimento de serviços gratuitos que incentivam a colaboração, cooperação e interactividade²⁵ – o utilizador *online* deixou de ser apenas um mero consumidor, para também ser um agente activo na colocação e difusão de conteúdos na Internet²⁶.

²³ Disso é exemplo, entre outros, a *Wikipédia* (www.wikipedia.com) cuja actualização da base de dados é feita em exclusivo pelos seus utilizadores que têm a possibilidade de introduzir novas entradas na base de dados, ou, simplesmente, de desenvolverem uma entrada já existente.

²⁴ Por exemplo, o *Facebook* (www.facebook.com) e o *Twitter* (www.twitter.com) permitem que o utilizador coloque conteúdos não só através de um computador, mas também através de um telemóvel, desde que este tenha, como é óbvio, acesso à Internet.

²⁵ Vide CARLISLE GEORGE e JACKIE SCERRI, *op. cit.*, p. 4. Poderíamos colocar a questão destes novos serviços da *web 2.0* não se considerarem no âmbito da definição de comércio electrónico, por serem serviços gratuitos para o utilizador. No entanto, em nosso entender, a definição actual de comércio electrónico não se deve cingir apenas aos serviços prestados mediante o pagamento de um preço. A maioria dos serviços da *web 2.0*, apesar de não exigirem o pagamento de um preço para serem utilizados, não deixam de ser prestados no âmbito de uma actividade económica, conseguindo os seus lucros através da publicidade que albergam nos seus *sites*. Tal como refere CARNEIRO DA FRADA, “ “Vinho novo em odres velhos?” – A responsabilidade civil das operadoras de Internet e a doutrina comum da imputação de danos”, in *Direito da Sociedade da Informação*, Vol. II, p. 14, “(...) a gratuidade das prestações que [os prestadores de serviços na rede] efectuam não é incompatível com o intencional de vantagens e recompensas no mercado.”. Pelo que, desde que o serviço possa ser enquadrado dentro de uma actividade económica, em nosso entender fará parte do comércio electrónico e estará sujeito aos seus princípios e normas, salvo disposição legal expressa em contrário.

²⁶ Apesar desta nova importância que, com a *web 2.0*, o utilizador passa a ter na colocação e difusão de conteúdos *online*, o mesmo ainda se inclui dentro da definição legal de consumidor que nos é dada pelo n.º 1 do artigo 2.º da Lei n.º 24/96, de 31 de Julho: os serviços de que o utilizador usufrui para colocar e difundir conteúdos são-lhe fornecidos normalmente por pessoas colectivas que exercem com carácter profissional uma actividade económica que visa a obtenção de benefícios (os prestadores de serviços intermediários em rede, como veremos *infra*).

1.3. Os conteúdos gerados por utilizadores

Por conteúdos gerados por utilizadores – CGU (ou, em linguagem anglo-saxónica, *User Generated Content – UGC*) – entendemos, como o próprio nome indica, conteúdos que são criados, colocados e partilhados na *www* pelos próprios utilizadores finais da mesma²⁷.

Este tipo de conteúdos é distinguível dos conteúdos gerados por um fornecedor de conteúdos, por três ordens de razões: em primeiro lugar, os CGU, geralmente, são conteúdos muito associados à pessoa do utilizador que os coloca em rede e, deste modo, não são, em regra, antecidos de nenhum controlo ou correcção para assegurar a sua qualidade, ao contrário dos segundos que costumam ser precedidos de um alto nível de supervisão e de segurança da respectiva qualidade, considerando-se estes últimos, à partida, mais confiáveis e credíveis do que os primeiros; em segundo lugar, a periodicidade de colocação na rede de conteúdos gerados por um utilizador em concreto é incerto, dependendo unicamente da vontade deste a decisão e o momento dessa colocação²⁸, ao contrário dos conteúdos gerados por um fornecedor de conteúdos que coloca conteúdos na rede com uma periodicidade regular e constante²⁹; finalmente, em terceiro lugar, a actividade de colocação de conteúdos na rede por utilizadores é feita, na maior parte das vezes, sem fins lucrativos, ao contrário dos conteúdos colocados pelos respectivos fornecedores que, geralmente, sendo pessoas colectivas inseridas no seio de uma actividade económica, o fazem com intuito lucrativo.

Por outro lado, os serviços *online* que permitem a colocação de conteúdos gerados por utilizadores são, na sua generalidade, *websites* cujo sucesso se encontra intimamente relacionado com a variedade dos conteúdos colocados pelos seus utilizadores, bem como com a partilha desse mesmo conteúdo. Por outro lado, os *websites* de CGU possuem uma atitude proactiva no sentido de encorajar os seus utilizadores a colocarem cada vez mais conteúdos e a partilharem o respectivo conteúdo³⁰.

Os serviços *online* que permitem a colocação e difusão de CGU na Internet podem, genericamente, dividir-se nas seguintes categorias:

²⁷ Vide ERIK VALGAEREN e NICOLAS ROLAND “Youtube and social networking sites – New kids on the block?” in *Google et les nouveaux services en ligne*, p. 208.

²⁸ Embora a entrada de um novo CGU na rede seja quase instantânea, quando tendo em conta a globalidade dos utilizadores que inserem conteúdos na *www*.

²⁹ O fornecedor de conteúdos não é mais do que um fornecedor de serviços, sendo que, neste caso, o serviço que presta é precisamente a criação e colocação de conteúdos *online*.

³⁰ Vejam-se, a título de exemplo, as inúmeras aplicações disponíveis no *Facebook* que, para serem utilizadas, obrigam a que o utilizador conceda na partilha de alguns elementos que possui na sua “página de perfil”, ou então os vídeos colocados no *Youtube* cuja popularidade aumenta consoante aumente o número de pessoas que visualize o vídeo.

- Disponibilização de espaço para alojamento e partilha de conteúdos: armazenamento e partilha de vídeos (são disso exemplo o *Youtube* e o *Myspace*); armazenamento e partilha de textos (por exemplo, o *Blogger* e o *Twitter*); armazenamento e partilha de fotos (por exemplo o *Flickr*);

- Disponibilização de espaço para a criação de bases de dados colectivas (como é disso grande exemplo a *Wikipedia*);

- Disponibilização de espaço para alojamento de ficheiros, para posteriormente serem descarregados por terceiros (por exemplo, o *Mediafire* ou o *Rapidshare*)

- Redes sociais – respeitantes à partilha de informações pessoais e /ou profissionais (tais como o *Facebook*, *Hi5*, ou o *Linkedin* – este último relativo à partilha de informações profissionais);

- *Software* de partilha de conteúdos entre computadores – respeitante ao já referido *software* P2P (por exemplo o *E-mule*, *BitTorrent*, entre outros).

Esta divisão é feita de acordo com as funções primárias de cada serviço, uma vez que, em termos práticos, cada serviço pode possuir outras finalidades, consoante o constante desenvolvimento do serviço – factor essencial da *web 2.0*. Por exemplo o *Blogger*, um serviço de criação e alojamento de blogues na *www* apesar de estar inicialmente formatado para permitir aos seus utilizadores escreverem textos e alojarem-nos nos servidores do serviço, hoje em dia permite o alojamento de ficheiros de vídeo e de música, bem como o *upload* de fotos³¹. Por outro lado, hoje em dia é bastante habitual assistir-se a uma própria partilha de conteúdos entre os diversos serviços³².

Quais são as razões que levam um utilizador a colocar conteúdos *online*? Estas são inúmeras e diversas, pelo que procedemos aqui a uma enumeração exemplificativa de algumas das principais razões³³:

- *Razões lúdicas*: Grande parte dos utilizadores coloca conteúdos na *web* para seu próprio divertimento e para o divertimento de outros utilizadores;

- *Razões informativas*: Alguns utilizadores colocam conteúdos de modo a informar o restante público quanto a um determinado assunto, podendo chegar a conteúdos que

³¹ Sobre os blogues e as questões particulares que suscitam na efectivação da responsabilidade civil na Internet vide o nosso “A Responsabilidade Civil pelo conteúdo da informação transmitida através de blogues”, in *Jusjournal* de 13 de Maio de 2010.

³² Por exemplo, é possível, no *Facebook*, colocar ligações para vídeos alojados no *site* do *Youtube* e visualizá-los através do *Facebook* sem necessidade de abrir a página do *Youtube*.

³³ Seguimos de perto a enumeração dada por CARLISLE GEORGE e JACKIE SCERRI, *op. cit.*, p. 4.

consubstanciam peças de verdadeiro jornalismo – e que são, muitas das vezes, até são utilizadas pelos tradicionais meios de comunicação social³⁴;

- *Razões sociais*: Muitos dos conteúdos colocados na *web* por utilizadores também se referem a causas sociais, divulgando e criando movimentos de ajuda social, de protecção dos animais, de ajuda humanitária, entre outros;

- *Razões ideológicas / políticas*: Os conteúdos colocados na *web* também podem servir para apoiar ou criticar determinadas ideologias e actuações políticas, bem como para campanhas eleitorais³⁵. De igual modo, a colocação de conteúdos *online* por utilizadores pode servir para denunciar comportamentos “eticamente duvidosos” por parte de agentes políticos³⁶;

- *Razões económicas*: Embora constitua uma minoria, alguns utilizadores também colocam conteúdos *online* com o fim de conseguirem vantagens pecuniárias, nomeadamente através de publicidade associada aos conteúdos que colocam em rede³⁷, utilizando, no fundo, o mesmo modo de financiamento próprio dos serviços da *web 2.0*;

- *Razões ilegais*: Por fim, os utilizadores podem colocar conteúdos *online* que, voluntária ou involuntariamente, prejudicam terceiros, tais como a colocação e disponibilização a terceiros de obras protegidas pelos direitos de autor, a criação e publicação de fotomontagens com figuras públicas conhecidas, a publicação de textos difamatórios, a criação e difusão *online* de vírus, entre muitos outros exemplos.

1.4. Balanço preliminar: A necessidade do Direito intervir no mundo digital

A Internet, em particular a *www* e a *web 2.0*, trouxe um novo paradigma de sociedade: uma sociedade global, sem fronteiras, interligada. Hoje assiste-se ao culminar do verdadeiro sentido da expressão “Sociedade da Informação”, com o livre acesso de todos e de cada um de

³⁴ São disso exemplo os vários vídeos de tragédias que são captadas por câmaras amadoras e depois são alojados no *Youtube* e, posteriormente, transmitidas pelos canais televisivos, como sucedeu, por exemplo, com o tsunami ocorrido em Março de 2011 e que afectou parte da costa territorial do Japão.

³⁵ Hoje em dia, é usual em eleições colocarem-se vídeos promocionais na *web* ou não se criarem perfis em redes sociais, o que vai para além da tradicional criação de uma *homepage*, como sucedia antes do “boom” da *web 2.0*.

³⁶ Destacamos, sem dúvida, o fenómeno do *Wikileaks*, não só pelo famoso vídeo tornado público do abate de jornalistas no Iraque por soldados norte-americanos, bem como pelo ainda mediático *cable case* relativo à divulgação de milhares de telegramas das embaixadas norte-americanas. Embora em nosso entender o *Wikileaks* seja, para todos os efeitos, um fornecedor de conteúdos (e não um mero utilizador), este é um exemplo bastante elucidativo do poder da *web* na divulgação de informações politicamente indesejadas (e cuja actuação, por conseguinte, também não se pode considerar ideologicamente neutra).

³⁷ Por exemplo, o *Blogger* permite aos seus utilizadores que coloquem no seu blogue publicidade da *Google* (curiosamente a proprietária do *Blogger*), atribuindo uma quantia pecuniária consoante o número de visualizações do blogue.

nós ao resto do Mundo. Como bem referem GARCIA MARQUES e LOURENÇO MARTINS, “A Sociedade da Informação – expressão que cada vez importa menos definir na medida em que se vai vivendo em maior escala – assenta pois sobre o uso óptimo das novas tecnologias da informação e da comunicação, em respeito pelos princípios democráticos, da igualdade e da solidariedade, visando o reforço da economia e da prestação de serviços públicos e, a final, a melhoria de qualidade de vida de todos os cidadãos”³⁸.

Assim, a Internet, hoje em dia, deve ser acessível a todos, constituindo, em nosso entender, um verdadeiro bem público. Todo o cidadão deve ter direito a aceder à Internet e a utilizá-la como bem entender. “A Sociedade da Informação tem de ser uma sociedade para todos”³⁹.

Durante algum tempo, pensou-se que a Internet seria um espaço alheio ao Direito, sem necessidade de qualquer tipo de regulamentação. A Internet seria, assim, uma *no man’s land* cujos efeitos, mesmo que nocivos, teriam de ser suportados por todos.

No entanto, depressa se constatou que a Internet não poderia ser um sector da sociedade alheia ao Direito. Na verdade, o mundo digital trouxe uma panóplia de situações que, pela sua própria natureza, careciam (e carecem) de ser legalmente regulamentadas. Como acertadamente aponta MIGUEL PEGUERA POCH, “as actividades que se levam a cabo através da rede apresentam, com grande frequência, uma vertente jurídica que não se pode desconhecer. Mediante as vias de comunicação electrónica próprias deste espaço virtual, transmite-se informação, tornam-se acessíveis conteúdos, produzem-se declarações de vontade, concluem-se e executam-se contratos, utilizam-se sinais distintivos, reproduzem-se criações intelectuais, levam-se a cabo pagamentos, exerce-se a liberdade de expressão com grande variedade de manifestações, faz-se publicidade directa, oferecem-se e prestam-se variadíssimos serviços...”⁴⁰.

Em concreto, no que ao nosso estudo diz respeito, se é verdade que a Internet e, em especial, os serviços da *web 2.0*. permitiram (e permitem) um aumento exponencial das possibilidades de manifestação da liberdade de expressão de cada utilizador individual, não menos verdade é que potenciaram as possibilidades de actuações ilegítimas através da rede, nomeadamente através da colocação e difusão na Internet de conteúdos ilícitos.

³⁸ *Op. cit.*, p. 41

³⁹ JOEL TIMÓTEO RAMOS PEREIRA, *Compêndio jurídico...*, p. 31

⁴⁰ Tradução livre nossa de MIGUEL PEGUEIRA POCH, “La exención de responsabilidad civil por contenidos ajenos en Internet”, in *Revista Aranzadi de Derecho y Proceso Penal*, n.º 8, p. 33, nota 14.

Assim, tornou-se necessária uma actuação do Direito no campo da responsabilização pelos actos ilícitos cometidos na rede. No que toca a conteúdos ilícitos colocados e difundidos na Internet, importará, antes de mais, fazer um levantamento dos vários intervenientes na colocação e difusão de conteúdos na Internet. Seguidamente, importará saber de que forma o sistema vigente da responsabilidade civil é, ou não, eficaz para ressarcir os lesados de danos provocados por aqueles conteúdos.

2. Os intervenientes na colocação e difusão de conteúdos na Internet

2.1. A dificuldade de criação de um critério estanque e uniforme para a sua concreta definição

Um dos primeiros problemas relativos à temática da Responsabilidade Civil por conteúdos ilícitos colocados e difundidos na Internet prende-se precisamente com a dificuldade de definir com rigor suficiente os sujeitos que actuam na Internet e que interagem (activa ou passivamente) com os conteúdos que são colocados em rede e aí circulam.

Mais difícil se torna a sua definição se atentarmos no facto de que a colocação e transmissão de conteúdos em rede se trata de uma operação complexa, que envolve a participação de inúmeros sujeitos, desde a sua colocação pela primeira vez na rede até à sua chegada ao local de destino⁴¹.

A título de exemplo, veja-se o caso de um utilizador que pretende colocar uma imagem armazenada na memória do seu computador numa página de Internet de modo a ser acessível a outros utilizadores. À primeira vista, poderíamos pensar que existem apenas dois intervenientes na colocação do conteúdo (a imagem) em rede: o remetente – neste caso o sujeito que coloca o conteúdo na página – e o destinatário – outro utilizador que visualiza a imagem na rede.

No entanto, esquecemo-nos que a página de Internet onde o utilizador coloca a imagem *online* se encontra alojada num servidor, que geralmente é propriedade de uma entidade terceira – uma prestadora de serviços informáticos – que, no entanto, permite o uso do seu servidor pelo utilizador em questão, permissão essa facultada pela existência de um contrato, normalmente gratuito, de prestação de serviços entre as duas partes. Encontramo-nos, então,

⁴¹ Sujeitos esses cuja existência é muitas vezes imperceptível, face à velocidade de transmissão dos conteúdos, fazendo da Internet uma enorme “nuvem” quanto à difusão de conteúdos na rede, como bem ilustra CHRIS REED, *Internet Law: Text and Materials*, p. 26.

perante três intervenientes na colocação e difusão do conteúdo: o remetente do conteúdo – o utilizador primitivo que coloca o conteúdo na página *web* – o intermediário de armazenamento do conteúdo – o prestador de serviço que armazena no seu servidor a página *web* e, conseqüentemente, os conteúdos que nela são colocados – e, por fim, o destinatário do conteúdo – que serão todos os sujeitos que visualizem a página *web* e a imagem ali colocada.

Todavia não nos podemos ficar por esta tripartição de intervenientes. Na verdade, olvidamos ainda outros prestadores de serviços intermediários na rede: referimo-nos aos que permitem que o sujeito primitivo aceda à página *web* onde quer colocar o conteúdo, bem como os intermediários que permitem o *upload* da imagem em formato compatível para ser colocada na página *web* (que poderá ou não ser o mesmo prestador de serviços que detém o servidor onde a página se encontra alojada) e, por fim, os intermediários que permitem o acesso dos restantes sujeitos ao conteúdo e à sua visualização e/ou *download*.

Por fim, ainda teremos de ter em conta toda a estrutura física de cabos e fios que permitem que todos os sujeitos *supra* referidos acessem à Internet e possam desempenhar as suas actividades na rede.

Em suma, como podemos constatar, no simples acto de colocação e difusão de um determinado conteúdo na rede intervém uma ampla categoria de sujeitos. Como caracterizar cada um deles?

2.2. Da delimitação em função do sujeito para a delimitação em função da actividade

Inicialmente, poderíamos cair na tentação de definir cada um dos intervenientes na difusão de um determinado conteúdo na rede em função da sua caracterização enquanto sujeito ao invés da sua caracterização pela actividade que o mesmo leva a cabo na Internet. No entanto, ao procedermos dessa forma, depressa chegaríamos à necessidade de reformular as definições.

Isto porque, na Internet, cada sujeito pode levar a cabo um infinito leque de actividades. Por outro lado, mais sentido fará definir os intervenientes na Internet de acordo com a actividade que, num caso em concreto, prosseguem, se atendermos a que, graças aos avanços da tecnologia, cada vez mais é permitido ao utilizador comum desenvolver actividades na

Internet que, há vinte anos atrás, apenas estavam ao alcance dos verdadeiros “gurus” informáticos⁴².

Por exemplo, um sujeito que coloque um conteúdo em rede também pode receber outros conteúdos que, por sua vez, não foram por ele colocados. De igual forma, um intermediário pode proceder à prestação de serviços de armazenamento, mas também pode prestar serviços de transporte de determinados conteúdos de um servidor para outro⁴³.

Logo, a sugestão de definição dos vários intervenientes na Internet que *infra* se expõe é feita consoante a actividade que cada interveniente desempenha no caso em concreto e não consoante a sua individualidade⁴⁴.

2.3. Modelo seguido

Desde já poderemos dividir os sujeitos intervenientes na Internet em três grandes grupos, consoante a actividade que exerçam no caso em concreto: os *intervenientes principais*; os *fornecedores de infra-estruturas de comunicação*; os *prestadores intermediários de serviços em rede*⁴⁵.

Os *intervenientes principais* são, como o próprio nome indica, os intervenientes para os quais o conteúdo que circule na Internet tem uma importância directa. Ou seja, estamos a falar da pessoa, singular ou colectiva, que coloca o conteúdo em rede e da pessoa, singular ou colectiva, que o recebe. Tradicionalmente estar-se-ia a falar do *fornecedor de conteúdos*⁴⁶, por um lado, em contraposição com o *utilizador* ou *consumidor final*, por outro. No entanto, no advento da *web 2.0*, como vimos *supra*⁴⁷, o utilizador deixou de ser um mero consumidor dos conteúdos colocados na rede, para também contribuir para a criação e difusão

⁴² Hoje, tal como já referimos *supra*, p. 23 ss., encontramos na idade da *web 2.0* e na época áurea dos conteúdos gerados e difundidos por utilizadores.

⁴³ Bastará pensar, por exemplo, nos prestadores de serviços de correio electrónico (*hotmail*, *gmail*, etc...): não só prestam serviços de transporte de informação (envio de *e-mails* da caixa de correio de um utilizador para a caixa de correio do destinatário), como também prestam serviços de armazenamento (na medida em que as caixas de correio que guardam a correspondência electrónica recebida encontram-se alojadas nos servidores dos prestadores de serviços).

⁴⁴ Neste sentido vide CLÁUDIA TRABUCO, “Conteúdos ilícitos e responsabilidade dos prestadores de serviços nas redes digitais”, in *Direito da Sociedade da Informação*, Vol. VII, p. 476 ss. e nota 5. Em sentido aparentemente diverso vide MENEZES LEITÃO, “A Responsabilidade Civil na Internet”, in *Direito da Sociedade da Informação*, Vol. III, pp. 157 ss.

⁴⁵ Seguimos, nesta parte, embora com algumas divergências, a proposta de divisão dos intervenientes na Internet sugerida por CHRIS REED, *Internet Law...*, pp. 24 ss.

⁴⁶ Expressão utilizada por MENEZES LEITÃO, “A Responsabilidade Civil...”, p. 158, para designar a “entidade que coloca conteúdos *online*, à disposição dos utilizadores da internet.”

⁴⁷ Vide pp. 23 ss.

dos mesmos. Assim, será mais correcto falar-se apenas em *utilizadores*, como *intervenientes principais* na rede, enquanto pessoas, singulares ou colectivas, simultaneamente geradores e consumidores de conteúdos na rede.

Em segundo lugar temos os *fornecedores de infra-estruturas de comunicação*. Estes são os proprietários dos cabos, redes de fios e todos os outros elementos físicos que permitem que todas as pessoas, singulares ou colectivas, se liguem à Internet e, por sua vez, permitem também que a informação circule entre os diversos objectos corpóreos informáticos (*hardware*), em suma, permitem a ligação global de todos os sistemas informáticos, controlando assim a “parte física” da “rede das redes”. O fornecimento de infra-estruturas de comunicação encontra-se intimamente ligado à actividade económica das chamadas empresas de telecomunicações, embora o objecto social destas se estenda para além do mero fornecimento de infra-estruturas, desenvolvendo também actividades de prestação intermediária de serviços em rede⁴⁸.

Em último lugar temos os chamados *prestadores intermediários de serviços em rede*⁴⁹. Estes prestadores de serviços, são, como o próprio nome indica, pessoas, singulares ou colectivas⁵⁰, que, intervindo de forma autónoma, permanente e organizada, permitem que um determinado conteúdo circule na Internet e, consequentemente, que o utilizador que o coloca *online* consiga transmiti-lo ao utilizador que o visualiza, a final⁵¹. Uma das principais características que está subjacente aos prestadores de serviços intermediários é a sua posição neutra face aos conteúdos que transmitem, isto é, não interferem na criação do conteúdo, limitando-se a proceder a um tratamento automático do mesmo no âmbito da actividade de prestação de serviços que exercem. Também é necessário notar, como faz CARNEIRO DA FRADA, que estes intermediários prestam os seus serviços normalmente com fins lucrativos⁵². A Directiva Europeia sobre o Comércio Electrónico (Directiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de Junho de 2000 – doravante DCE) não logrou definir o que eram os prestadores de serviços intermediários em rede, omissão essa que o

⁴⁸ Veja-se, por exemplo, o caso do grupo *Portugal Telecom* que possui um leque de prestação de serviços intermediários, nomeadamente através da marca *Sapo*.

⁴⁹ Também apelidados de *Operadoras de Internet*, noção empregue por CARNEIRO DA FRADA, “ “Vinho novo em odres velhos?...”, pp. 7 ss.

⁵⁰ Embora na maioria das vezes sejam pessoas colectivas, pela própria natureza da actividade que exercem, como veremos *infra*.

⁵¹ A definição que agora se apresenta corresponde à conjugação das definições destes intervenientes dadas por CARNEIRO DA FRADA, “ “Vinho novo em odres velhos?...”, p. 10 e CHRIS REED, *op. cit.* p. 27.

⁵² “ “Vinho novo em odres velhos?...”, p. 10. Isso não significa necessariamente que o contrato de prestação de serviços celebrado entre os intermediários e o fornecedor de conteúdos seja celebrado a título oneroso, mas simplesmente que a sua actividade é realizada com o objectivo de obtenção de lucro, muitas vezes até através de anúncios publicitários presentes nas páginas e nos serviços que prestam, conforme se referiu *supra*, p. 24.

legislador português, na transposição daquela, procurou colmatar, pelo que, nos termos do disposto no n.º 5 do artigo 4.º do Decreto-Lei n.º 7/2004, alterado pelo Decreto-Lei n.º 62/2009, de 10 de Março, denominado Regime Jurídico do Comércio Electrónico (RJCE), “Prestadores intermediários de serviços em rede» são os que prestam serviços técnicos para o acesso, disponibilização e utilização de informações ou serviços em linha independentes da geração da própria informação ou serviço.”, definição esta que consubstancia os traços essenciais destes intervenientes na rede que *supra* referenciámos.

Dentro deste último grupo será ainda necessário delinear uma diferenciação entre os vários intermediários, consoante a actividade que os mesmos exerçam ou estejam a exercer num caso concreto. Assim, teremos⁵³:

Os fornecedores de acesso: Se com o seu serviço permitem o acesso dos intervenientes principais à rede. Estes intermediários distinguem-se dos fornecedores de *infra-estruturas de comunicação*, uma vez que aqueles actuam na própria Internet em si, na natureza incorpórea que a constitui, ao passo que estes actuam, como referimos, no exterior da Internet, no controlo dos objectos corpóreos que permitem a existência da rede.

Os fornecedores de transporte: Se com o seu serviço procedem à transmissão dos conteúdos na rede. Este fornecimento encontra-se presente em todas as actividades de envio ou descarregamento de conteúdos, bem como no transporte de conteúdos entre diversas bases de dados e/ou servidores.

Os fornecedores de armazenamento: Se com o seu serviço permitem aos intervenientes principais o uso de determinado espaço do seu servidor, para que estes o utilizem, ficando o intermediário também responsável pela armazenagem dos conteúdos ali colocados. A armazenagem em si pode ser temporária ou principal. A armazenagem temporária consiste no “armazenamento temporário de cópias das páginas e serviços consultados frequentemente pelos utilizadores, permitindo desta forma um acesso mais rápido aos mesmos, o que apresenta desde logo a vantagem de descongestionamento da rede e, consequentemente, um melhor desempenho das suas tarefas.”⁵⁴, também denominado de *caching* ou *mirroring*⁵⁵ A armazenagem principal trata-se, por seu turno, da armazenagem das informações e/ou conteúdos nas próprias páginas e outros serviços onde eles foram colocados primariamente. A

⁵³ Seguimos aqui, embora com divergências, a sistematização adoptada por MENEZES LEITÃO, “A Responsabilidade Civil...”, p. 158.

⁵⁴ Vide CLÁUDIA TRABUCO, “Conteúdos ilícitos...”, p. 489.

⁵⁵ Técnica usada, por exemplo, para a difusão do site da empresa Wikileaks. O *mirroring* trata-se de uma técnica que permite efectuar uma cópia idêntica de um determinado *site* e alojá-la num servidor distinto do que aloja o *site* primitivo.

distinção entre a actividade de armazenagem temporária e principal é importante, uma vez que ambas estão sujeitas a diferentes graus de “*irresponsabilidade*”, como veremos *infra*⁵⁶.

No que toca à responsabilidade por conteúdos ilícitos colocados e difundidos em rede, assumem particular relevância os papéis dos *utilizadores* e, por outro lado, dos *prestadores de serviços intermediários em rede*.

Abstemo-nos de abordar a eventual responsabilidade dos *fornecedores de infra-estruturas de comunicação* pelos conteúdos ilícitos colocados e difundidos pela Internet, uma vez que estes, de acordo com a definição que apresentámos, não possuem qualquer intervenção activa na colocação e difusão de conteúdos ilícitos na rede, sendo detentores dos meros cabos físicos por onde a informação (e, consequentemente, os conteúdos) circula.

Finalmente, importará ainda referir o papel do lesado, enquanto sujeito que sofre um dano em virtude de um conteúdo colocado e difundido na Internet. O lesado tanto poderá ser um outro utilizador da Internet que, ao aceder ao conteúdo ilícito, sofre o dano (por exemplo, pelo download de um conteúdo que possui um *vírus* escondido), como poderá ser um terceiro que não acede ao conteúdo ilícito directamente (por exemplo, pense-se na publicação numa rede social de uma foto de uma pessoa pública que não é cliente dessa mesma rede social). Importará, contudo, analisar a sua conduta de forma a apurar se o seu comportamento poderá levar a uma eventual exclusão ou limitação da responsabilidade civil dos agentes responsáveis pela colocação e difusão do conteúdo ilícito.

Assim, iremos, primariamente, analisar as traves-mestras da responsabilidade civil dos utilizadores enquanto agentes responsáveis pela colocação e difusão de um conteúdo ilícito na Internet e, em segundo plano, da necessidade de responsabilização cível dos intermediários que promovam a difusão dos conteúdos ilícitos pela rede.

⁵⁶ Vide pp. 84 ss

CAPÍTULO II

PONTOS CRÍTICOS NA DETERMINAÇÃO DA RESPONSABILIDADE CIVIL DO UTILIZADOR QUE COLOCA E DIFUNDE CONTEÚDOS ILÍCITOS NA INTERNET

3. Ponto prévio: Breve referência à dogmática comum da responsabilidade civil

3.1. A noção de responsabilidade civil

Antes de nos debruçarmos sobre os problemas específicos que se levantam ou poderão levantar na imputação de um dano ocorrido pela colocação e difusão de um conteúdo ilícito na Internet, caberá recordar algumas noções elementares da dogmática comum da responsabilidade civil⁵⁷.

Por responsabilidade civil entende-se a imputação dos danos provocados numa determinada esfera jurídica a outra esfera jurídica diversa daquela, desde que verificados determinados requisitos.

É habitual distinguir-se entre responsabilidade civil obrigacional e responsabilidade civil extraobrigacional. Na primeira verifica-se a violação de uma obrigação, enquanto que na segunda existe uma violação de direitos absolutos ou de normas de protecção, que, independentemente da licitude da conduta, causam danos a outrem⁵⁸.

Hoje em dia, no entanto, constata-se que a divisão da responsabilidade civil em compartimentos estanques já não faz sentido, na medida em que assistimos a um proliferar de situações dúbias cujo enquadramento jurídico, do ponto de vista da responsabilidade civil, aquiliana ou obrigacional, não é satisfatório. Assiste-se então à emergência de responsabilidades intermédias, também denominadas de “terceiras vias”, cuja fonte não se baseia nem no delito, nem no contrato⁵⁹.

⁵⁷ Sobre o tema em geral vide ALMEIDA COSTA, *Direito das Obrigações*, p.557ss., ANTUNES VARELA, *Das Obrigações em Geral*, Vol. I, p. 518ss, CARNEIRO DA FRADA, *Direito Civil – Responsabilidade Civil: O método do caso*, pp. 60 ss., MENEZES CORDEIRO, *Direito das Obrigações*, 2ºvol., p.301 ss. e *Tratado de Direito Civil Português : II – Direito das Obrigações*, Tomo III, pp. 285 ss., MENEZES LEITÃO, *Direito das Obrigações*, Vol. I, p.287ss. e RIBEIRO DE FARIA, *Direito das Obrigações*, vol. I, p.410ss.

⁵⁸ RIBEIRO DE FARIA, *Direito...*, vol. I, p.411

⁵⁹ São exemplos da chamada “terceira via” a *culpa in contrahendo*, o contrato com eficácia de protecção para terceiros ou, até, a responsabilidade pela confiança, esta última exaustivamente desenvolvida por CARNEIRO DA FRADA, *Teoria da Confiança e Responsabilidade Civil*.

No que ao nosso estudo diz respeito, a colocação e difusão de conteúdos ilícitos na Internet implicará, regra geral, situações de responsabilidade civil extraobrigacional, na medida em que, na maioria das situações, não existe qualquer relação especial pré-existente entre lesante e lesado⁶⁰. Assim, daremos enfoque no nosso estudo a esta vertente da responsabilidade civil, sem, no entanto, deixarmos de invocar a responsabilidade civil obrigacional ou fazermos alusão à “terceira via” nos momentos que entendermos oportunos⁶¹.

3.2. Pressupostos da responsabilidade civil

Nos termos do n.º1 do artigo 483.º do Código Civil (CC) “Aquele que, com dolo ou mera culpa, violar ilicitamente o direito de outrem ou qualquer disposição legal destinada a proteger interesses alheios fica obrigado a indemnizar o lesado pelos danos resultantes da violação.” Por sua vez, o artigo 798.º CC refere que “o devedor que falta culposamente ao cumprimento da obrigação torna-se responsável pelo prejuízo que causa ao credor.”, referindo o n.º2 do artigo 799.º deste diploma legal que “a culpa é apreciada nos termos aplicáveis à responsabilidade civil.”

Quer nos encontremos no âmbito da responsabilidade civil extraobrigacional quer no âmbito da responsabilidade civil obrigacional, é necessário que se demonstre o preenchimento de uma série de requisitos para que possa surgir na esfera jurídica do lesante a obrigação de indemnizar o lesado. A enumeração do que sejam tais requisitos sempre foi, e é, questão debatida no seio da doutrina nacional e que, atendendo à circunscrição do tema de estudo, não caberá nestas páginas desenvolver. Apenas diremos que seguimos a doutrina da Escola de Coimbra, que assenta numa penta-repartição dos requisitos da responsabilidade civil^{62 63}. Percebemos algumas das críticas que lhe são feitas, nomeadamente o facto de ser aplicável apenas à responsabilidade civil por factos ilícitos, mas conforme referimos, será este o tipo de

⁶⁰ Como, p.e., a existência de um vínculo contratual entre as partes ou uma relação de confiança entre elas.

⁶¹ Vide, a respeito da responsabilidade obrigacional, o ponto 14, *infra*, pp. 106 ss.

⁶² Vide, entre outros, ALMEIDA COSTA, *op. cit.*, p. 557; ANTUNES VARELA, *op. cit.*, p. 526; RIBEIRO DE FARIA, *op. cit.*, p. 413; MENEZES LEITÃO, *Direito das Obrigações*, p. 287.

⁶³ Ao contrário da doutrina sufragada pela Escola de Lisboa, que assenta numa repartição sintética entre dano e imputação. Vide, quanto a este respeito, MENEZES CORDEIRO, *Direito das Obrigações*, p. 301 ss. CARNEIRO DA FRADA, *Direito Civil - Responsabilidade Civil...*, p. 64, atendendo às críticas que se podem apontar quer à orientação descritiva que subjaz à Escola de Coimbra, quer às críticas que se podem apontar à orientação sintética que subjaz à Escola de Lisboa, opta por um “meio-termo”, baseando-se na enunciação de “requisitos genéricos”, traduzidos numa situação de responsabilidade, uma forma de imputação, um dano e um nexo de causalidade.

responsabilidade civil que estará mais em enfoque no nosso estudo⁶⁴. Apraz-nos tal critério por ser preferível à enumeração sintética “dano-imputação”, para efeitos de explicação das várias questões suscitadas na aplicação do instituto da responsabilidade civil aos conteúdos colocados e difundidos na Internet. Por fim, o critério da Escola de Coimbra continua, a nível prático, a ser o mais seguido pela jurisprudência portuguesa.

Assim, de acordo com o critério adoptado, existem cinco pressupostos para que exista responsabilidade civil: o facto voluntário do agente; a ilicitude; a culpa; o dano; e, finalmente, o nexo de causalidade entre o facto e o dano.

Por facto voluntário do agente devemos considerar toda a “conduta humana pensável como controlável pela vontade e que, nessa medida, pode ser imputada objectivamente”⁶⁵. Assim, no âmbito da nossa investigação, o facto voluntário do agente tratar-se-á da colocação e/ou difusão de um determinado conteúdo na Internet.

Iremos agora analisar de que forma tais conteúdos serão considerados ilícitos na rede, bem como que questões relevantes se poderão colocar no preenchimento dos três restantes requisitos da responsabilidade civil: a culpa do agente, o dano causado e o nexo de causalidade entre o dano e a colocação / difusão de conteúdos *online*.

Por uma questão de facilidade e clareza de exposição dogmática, optámos por individualizar as questões relacionadas com cada um dos requisitos da responsabilidade civil, de acordo com o critério adoptado; no entanto, saliente-se que, na prática, os requisitos da responsabilidade civil sempre terão de ser analisados em conjunto e como um todo incindível.

4. A ilicitude dos conteúdos colocados e difundidos na Internet

4.1. A dificuldade na determinação da ilicitude na Internet: Breve alusão ao carácter transnacional da Internet

A Internet, como espaço global de criação e partilha de informação, é, pela sua própria natureza, uma realidade transnacional, o que acaba por colocar sérios problemas jurídicos quanto à determinação da lei aplicável para uma determinada situação fáctica, nomeadamente

⁶⁴ Acrescente-se também que, como faz MENEZES CORDEIRO, *Tratado de Direito Civil...*, p. 433, “(...) a responsabilidade civil tem uma efectiva matriz delitual.”, pelo que, também por esta via se justifica o acolhimento daquele modelo.

⁶⁵ RIBEIRO DE FARIA, *Direito...*, Vol. I, p. 413

no que toca à determinação da ilicitude do conteúdo. Isto porque os conteúdos que são colocados na Internet se tornam instantaneamente acessíveis em qualquer lugar do mundo, bem como a sua difusão se torna igualmente generalizada e de maneira extremamente rápida⁶⁶.

Assim, o que é ilícito em Portugal não será necessariamente ilícito noutros países⁶⁷. Incumbirá então, sempre que se aborde a problemática da responsabilidade civil por conteúdos colocados e difundidos na Internet, procurar determinar a lei aplicável, de modo a conseguir averiguar se, à luz dessa lei, o conteúdo é, ou não, ilícito e se se encontram reunidos todos os pressupostos para a responsabilização do agente.

Tal averiguação diz respeito à ciência do Direito Internacional Privado e o seu estudo aprofundado, não obstante o manifesto interesse, extravasa o âmbito do nosso estudo, bem como os limites formais do mesmo⁶⁸.

No entanto, não deixaremos de referir que, relativamente a esta matéria, assume relevância o Regulamento n.º 864/2007 do Parlamento Europeu e do Conselho, de 11 de Julho de 2007, também apelidado de Regulamento Roma II, tendo entrado em vigor para todos os Estados-Membros da União Europeia, com excepção da Dinamarca, no dia 11 de Janeiro de 2009. Este regulamento visou harmonizar as normas de conflitos existentes nos Estados-Membros relativamente a questões de responsabilidade civil extraobrigacional, limitando assim o chamado *forum shopping*.

O Regulamento Roma II é aplicável às obrigações extracontratuais em matéria civil e comercial quando envolvam um conflito de leis, pelo que se torna manifesta a sua aplicabilidade aos hipotéticos casos de responsabilidade civil que se possam suscitar pela colocação de conteúdos ilícitos na Internet.

Geralmente não existirá qualquer convenção entre lesante e lesado ao nível do ordenamento jurídico aplicável para regular casos de responsabilidade civil extraobrigacional, na medida em que estes não têm nenhuma relação profissional, negocial ou de confiança entre si. Assim, aplicar-se-á o regime geral referido no Regulamento, que será a *lex loci damni*, a

⁶⁶ Neste sentido vide MARIO E. CLEMENTE MEORO e SANTIAGO CAVANILLAS MÚGICA, *Responsabilidad civil y contratos en internet – su regulación en la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico*, p. 35.

⁶⁷ Embora certos e determinados tipos de conteúdos terão uma concepção ilícita na generalidade dos países, pelo menos, dos mais desenvolvidos, tais como conteúdos relacionados com a pornografia infantil, actos de xenofobia, terrorismo, entre outros.

⁶⁸ Para um desenvolvimento aprofundado da lei aplicável a questões de Responsabilidade Civil por actos praticados através de redes de comunicações electrónicas vide, por todos, DÁRIO MOURA VICENTE, *Direito Internacional Privado: Problemática internacional da Sociedade da Informação*, em particular pp. 304 ss.

Lei do país onde ocorreu o facto danoso⁶⁹. Só assim não será se ambas as partes tiverem a sua residência habitual no mesmo país, caso em que será a Lei desse país a aplicável⁷⁰. Ressalvam-se os casos em que estiver em causa a violação de direitos de propriedade intelectual, em que será competente a Lei do país para o qual a protecção é reivindicada⁷¹, bem como os casos de concorrência desleal, em que a Lei competente será a do país em que as relações de concorrência ou os interesses colectivos dos consumidores sejam afectados ou sejam susceptíveis de ser afectados⁷².

Infelizmente, o Regulamento Roma II exclui do âmbito da sua aplicação matérias que, como veremos *infra*, constituem grande parte dos bens jurídicos geralmente violados por força da colocação e difusão de conteúdos ilícitos. Ficam excluídas, assim, do âmbito de aplicação do Roma II as matérias relacionadas com a violação da vida privada e dos direitos de personalidade.

Nestas matérias, não compreendidas pelo Regulamento, aplicar-se-á o regime geral previsto nos termos do disposto no artigo 45.º do CC. A norma de conflitos portuguesa não é muito diferente da regra geral prevista no Regulamento Roma II. Desde logo, nos termos do disposto no n.º 3 do seu artigo 45.º, se lesante e lesado tiverem a mesma nacionalidade, ou na falta dela, a mesma residência habitual, a Lei aplicável será a da nacionalidade ou a da residência comum. De resto, a responsabilidade extraobrigacional é regulada pela Lei do Estado onde decorreu a principal actividade causadora do prejuízo e, no caso de responsabilidade por omissão, é aplicável a Lei do lugar onde o responsável deveria ter agido, nos termos do disposto no n.º 1 do artigo 45.º.

Porém, no âmbito da matéria em estudo na presente tese, releva, para efeitos de determinação do ordenamento jurídico aplicável, o disposto no n.º 2 do artigo 45.º do CC, que dispõe que se a Lei do Estado onde se produziu o efeito lesivo considerar responsável o agente, mas não o considerar como tal a Lei do país onde decorreu a sua actividade, é aplicável a primeira Lei, desde que o agente devesse prever a produção de um dano, naquele país, como consequência do seu acto ou omissão. Isto porque, na maior parte das vezes, pelo menos no que toca a danos que se produzam na esfera jurídica de cidadãos portugueses residentes em Portugal, caso não seja possível identificar o agente responsável pelo facto e

⁶⁹ Cfr. artigo 4.º n.º1 do Regulamento.

⁷⁰ Cfr. artigo 4.º n.º2 do Regulamento.

⁷¹ Vide artigo 8.º n.º1. Para um enquadramento histórico da problemática da lei aplicável a violações de propriedade intelectual vide DÁRIO MOURA VICENTE, “Lei aplicável à responsabilidade pela utilização ilícita de obras disponíveis em redes digitais”, in *Direito da Sociedade da Informação*, Vol. III, pp. 169 ss.

⁷² Vide artigo 6.º n.º1.

seja necessário responsabilizar o prestador de serviços intermediários cujo sistema foi utilizado para a prossecução do acto ilícito⁷³, não raras vezes a actividade do prestador não será exercida no país onde se produziu o dano, *in casu*, Portugal.

Assim, parece-nos que, *prima facie*, a Lei do ordenamento jurídico português será, na maioria das vezes, aplicável a questões relacionadas com a responsabilidade civil por conteúdos colocados e difundidos na Internet. Questão diversa será a de saber se, na prática, a decisão dos tribunais portugueses será validamente reconhecida noutro país, *maxime*, nos Estados Unidos da América. Saliente-se, a título de exemplo dessa dificuldade, um polémico caso que se passou em França, onde o prestador de serviços intermediários *Yahoo!Inc.* foi condenado pelo *Tribunal de Grande Instance* de Paris a impedir o acesso, a partir de França, aos leilões do seu *site* (*www.yahoo.com*) onde se encontrava à venda uma série de objectos, colocados em leilão por utilizadores anónimos, relativos ao regime político do nacional-socialismo. Posteriormente, a sentença foi reenviada para os Estados Unidos da América, a fim de ser executada, em virtude da *Yahoo!Inc.* se encontrar domiciliada em San José, California. Não obstante, o *United States District Court for the Northern District of Califórnia* de San Jose não executou a sentença, por entender que a mesma era contrária à Primeira Emenda à Constituição Norte-Americana⁷⁴. O tribunal entendeu que se encontrava dentro dos limites da liberdade de expressão a venda de objectos referentes a qualquer ideologia política, inclusive quando referente ao nazismo⁷⁵.

Assim, torna-se claro que ainda existe um longo caminho a percorrer no que toca à harmonização internacional dos conteúdos lícitos e ilícitos colocados na Internet, harmonização essa que é perene atento o carácter eminentemente transnacional da Internet.

Feito este ponto prévio necessário, por uma questão de “visão de conjunto” da problemática, no nosso estudo, ao referirmo-nos a conteúdos ilícitos, teremos em conta o regime aplicável em Portugal, assim como será o mesmo o tido primariamente em conta⁷⁶ relativamente ao estudo das questões de responsabilidade civil que se levantam nesta sede, não obstante a referência a normativos e correntes jurisprudenciais de outros ordenamentos jurídicos que a natureza e o caminho da investigação em curso a isso obrigue.

⁷³ Situação que iremos estudar mais detalhadamente no capítulo III, *infra*, p.71

⁷⁴ Referente à Liberdade de Expressão.

⁷⁵ *Yahoo! Inc. v. La Ligue Contre el Racisme el L'Antisemitisme* (2001). *Apud* DÁRIO MOURA VICENTE, *Direito Internacional...*, pp. 338 ss.

⁷⁶ Bem como os diplomas comunitários do qual o regime português surge.

4.2. O conteúdo ilícito – Delimitação do conceito

Neste estudo, ao referirmo-nos a conteúdo ilícito, estamos a considerar a informação digital que, uma vez colocada e/ou divulgada na Internet, viola o direito de outrem ou uma disposição legal destinada a proteger interesses alheios⁷⁷. No entanto, não poderemos considerar o conteúdo ilícito *per se*, pois para que tal conteúdo seja considerado ilícito, regra geral, há que atender igualmente à conduta do agente na relação com esse mesmo conteúdo. Apenas equacionando a conduta do agente poderemos concluir pela ilicitude do conteúdo⁷⁸. Assim, por exemplo, um texto sobre determinada pessoa apenas será ofensivo do seu bom nome e, portanto, ilícito, quando publicado e divulgado através de um blogue e não quando se encontre guardada no disco rígido do computador do seu autor; de igual forma, um filme adquirido por um determinado consumidor não será em si mesmo ilícito, mas já o será se for disponibilizado a vários utilizadores de Internet, através de *software* P2P, sem o consentimento do autor do filme.

Assim, sempre que ao longo do presente estudo, nos referirmos a conteúdos ilícitos estamos a referir-nos não ao conteúdo em si, mas sim ao conteúdo e ao desvalor da conduta do agente no tratamento do conteúdo referido na Internet.

Tendo em conta que “o que é ilícito fora da rede permanece ilícito dentro da rede”⁷⁹, as várias formas de que se pode revestir a ilicitude dos conteúdos *online* não serão substancialmente diferentes das da ilicitude dos conteúdos *off-line*. Assim, o meio utilizado – a Internet – no que diz respeito à ilicitude, é neutro, não trazendo nada de novo à aplicação da dogmática comum da responsabilidade civil.

Uma vez que, conforme referido, a colocação e difusão de conteúdos ilícitos na rede consubstanciará, a maioria das vezes, situações de responsabilidade civil aquiliana, caberá fazer uma súmula das principais violações de direitos subjectivos que podem ocorrer por força de tal actuação na rede.

⁷⁷ Que são, no fundo, as formas de que pode revestir a ilicitude, nos termos do disposto no artigo 483.º n.º1 do CC

⁷⁸ Estaremos aqui a analisar o desvalor da conduta, por contraposição ao desvalor de resultado. *Vide*, a este respeito, MENEZES CORDEIRO, *Tratado de Direito Civil...*, pp. 437 ss.

⁷⁹ Assim se exprimiu a Comissão Europeia na sua comunicação sobre os conteúdos ilegais e nocivos na Internet, no ano de 2000.

4.3. As potenciais violações de direitos subjectivos efectuadas por conteúdos colocados e difundidos na Internet

4.3.1. Violação de direitos de personalidade

a) O direito à honra e ao bom nome

A Internet é um mecanismo da liberdade de expressão individual por excelência. No entanto, a liberdade de expressão, como qualquer outro direito individual da pessoa, tem limites. Efectivamente, no suposto uso da liberdade de expressão na Internet, *maxime* através de *posts* em *blogues*, comentários nas *redes sociais*, ou partilha de artigos e de opiniões, é frequente que tais actos traduzam uma ofensa ao crédito ou ao bom nome de outrem.

A par dos direitos de autor, o crédito e o bom nome de uma determinada pessoa são os direitos de personalidade frequentemente mais lesados na Internet. Isso explica-se pela natural apetência das plataformas da *web 2.0*, em particular dos *blogues* e outros serviços, para a expressão da opinião do utilizador.

É, no entanto, necessário delimitar que tipo de opiniões é que é susceptível de ofender o crédito e o bom nome. O legislador apenas considera que serão ilícitos os comportamentos violadores do bom nome e do crédito quando estes consubstanciem afirmações ou declarações de facto⁸⁰, daí que se encontrem excluídos os juízos de valor ou meras opiniões, uma vez que estas estão integralmente legitimadas pelo direito fundamental à liberdade de expressão⁸¹. Com especial destaque, poderemos colocar neste campo (dos juízos valorativos ou meras opiniões) o comentário político, as análises técnico-científicas e mesmo a sátira e a paródia⁸². No entanto, e em especial no que toca à sátira, o facto de ela estar excluída das ofensas ao bom nome ou ao crédito de outrem não interfere com a possibilidade de que exista uma responsabilidade de quem a pratica, nomeadamente por violação de direitos de personalidade de outrem, aplicando conjuntamente os arts. 70º e 483º do C.C⁸³.

Existindo uma ofensa ao bom nome ou ao crédito de outrem, em princípio só os lesados pelas afirmações feitas poderão ter direito a uma indemnização. No entanto, mesmo que o agente apenas tenha querido ofender determinadas pessoas, ele pode, igualmente, ser

⁸⁰ Neste sentido, FILIPE ALBUQUERQUE MATOS, *A responsabilidade civil por ofensa ao crédito ou ao bom nome*, p. 223

⁸¹ *Idem*, p. 260 e n.514.

⁸² Para mais desenvolvimentos sobre as circunstâncias em que estes tipos de opiniões se manifestam em confronto com o art. 484º do CC *Vide* ALBUQUERQUE MATOS, *op. cit.*, p.261 ss.

⁸³ *Idem*, p. 272.

obrigado a indemnizar outras que se sintam atingidas pela afirmação de tais factos, desde que exista uma conexão entre os danos causados e aqueles factos, à luz da formulação negativa da doutrina da causalidade adequada⁸⁴. Em especial na Internet, a possibilidade de existirem mais ofendidos do que aqueles inicialmente configurados pelo autor dos factos danosos é uma constante, devido à ampla capacidade de difusão de informação na rede.

b) O direito à reserva da intimidade da vida privada

A Internet é também um local por excelência apto a violar a reserva da intimidade da vida privada de uma pessoa. “*The right to be let alone*”⁸⁵, previsto no artigo 80.º do C. C., tem um conteúdo variável, sendo que as possíveis lesões desse direito terão de ser analisadas em concreto. De facto, como aponta PAULO MOTA PINTO, “(...) além da própria noção de vida privada ser, em certa medida, dependente do indivíduo, é também função das valorações de cada formação social”⁸⁶. Por isso, apesar de aquilo que será a intimidade de cada um ter uma índole subjectiva, ela tem também uma componente objectiva, dada pelas valorações sociais existentes.

Poderemos ver como claras violações da reserva da intimidade da vida a obtenção de dados pessoais sem autorização do respectivo titular, nomeadamente através da aposição de *cookies*⁸⁷ nos sites visitados pelo lesado, e, por outro lado, através da divulgação de informações⁸⁸, fotos ou vídeos⁸⁹ de índole privada e pessoal.

c) O direito à imagem

O direito à imagem, previsto no artigo 79.º do CC, é um direito de personalidade intimamente ligado ao direito à reserva sobre a intimidade da vida privada. Com efeito, “ (...) o direito à imagem, é, em primeiro lugar, o direito ao resguardo, isto é, o direito de

⁸⁴ Acompanhamos, nesta parte, a opinião de ALBUQUERQUE MATOS, *op. cit.*, p. 304 ss.

⁸⁵ Expressão de LOUIS BRANDEIS, *apud* PAULO MOTA PINTO, “O Direito à Reserva sobre a intimidade da vida privada”, in *Boletim da Faculdade de Direito* [separata], vol. LXIX.

⁸⁶ Vide PAULO MOTA PINTO, *op. cit.*, p. 527.

⁸⁷ O *cookie* é, nas palavras de JOEL TIMÓTEO RAMOS PEREIRA, *Compêndio jurídico...*, p. 1032, um “ (...) pequeno arquivo que fica armazenado no computador do utilizador e guarda todas as informações importantes sobre a sua navegação. O cookie permite que um sítio tenha um histórico da navegação do utilizador e, assim, personalize o conteúdo do sítio de acordo com o perfil de cada Internauta, mas também pode ser perigoso na medida em que o responsável pelo sítio pode ficar a conhecer determinadas preferências e informações de carácter pessoal do utilizador.”. Pode, inclusive, ser utilizado para a obtenção de dados informáticos pessoais, tais como a *password* de uma conta de *e-mail* ou de outro serviço da Internet subscrito pelo lesado.

⁸⁸ Como informações sobre a saúde, vida amorosa ou passado de uma determinada pessoa, entre outras.

⁸⁹ Sendo que a publicação de fotos ou vídeos também poderá resultar numa violação do direito à imagem, como veremos *infra*.

privacidade.”⁹⁰. Assim, nos termos do disposto no n.º1 do referido artigo 79.º, o retrato de uma pessoa não pode ser exposto, reproduzido ou lançado no comércio sem o consentimento dela.

O direito à imagem pode ser violado na Internet, desde logo através da circulação de ficheiros contendo fotos ou imagens de uma determinada pessoa, sem o seu consentimento. De igual forma assume particular relevância actual a gravação de vídeos através de telemóveis, expondo indivíduos, e a sua posterior publicações em *sites* de partilha de vídeos (como o *Youtube*) ou em redes sociais (como o *Facebook*)⁹¹.

Outro tipo de violações ocorrem não pela simples divulgação de uma determinada foto ou imagem, mas da deturpação da mesma, através de modificações em programas de computador específicos, dando origem a fotomontagens, muito comuns, por exemplo, para colocar fotografias de caras de celebridades em corpos nus⁹². Neste âmbito, permitimo-nos dar destaque a um muito polémico *site* português, intitulado “Fototanga”, onde eram colocadas fotos de figuras públicas portuguesas adulteradas com recurso à elaboração de fotomontagens⁹³.

Na ponderação do facto de estarmos perante, ou não, uma violação do direito à imagem, sempre se terá de ter em conta o disposto no n.º 2 do referido artigo 79.º do CC, na medida em que consagra causas justificativas da publicitação de imagens sem o consentimento do visado nas mesmas: quando assim o justifiquem a notoriedade da pessoa retratada, o cargo que desempenhe, exigências de polícia ou de justiça, finalidades científicas, didácticas ou culturais; ou quando a reprodução da imagem vier enquadrada na de lugares públicos (v.g. a fotografia panorâmica de uma rua de determinada cidade), ou na de factos de interesse público (v.g. a fotografia de uma conferência de imprensa do governo), ou que

⁹⁰ Vide JOEL TIMÓTEO RAMOS PEREIRA, *Compêndio jurídico...*, p. 17.

⁹¹ Muitos dos aludidos casos, além de violarem o direito à imagem de todos ou alguns dos visados, são também incitadores de comportamentos contrários aos bons costumes ou até incitadores à prática de actos ilícitos. Veja-se, a título de exemplo, o caso mediático da filmagem numa sala de aula da aluna que desobedeceu violentamente à sua professora quando esta lhe ordenava a entrega do telemóvel que estava a servir de distração à aluna ou, mais recentemente, a filmagem de uma cena de agressão física de duas jovens a uma terceira. Com efeito, situações como as descritas demonstram uma clara falta de sensibilidade dos seus autores (maioritariamente menores de 18 anos) para a gravidade dos factos que tais vídeos relatam.

⁹² A este respeito já se produziu jurisprudência nacional relativamente à violação do direito à imagem através de uma fotomontagem levada a cabo na Internet, tendo o réu sido condenado a pagar à lesada uma indemnização por danos morais, devido a ter colocado numa página de Internet uma fotomontagem, utilizando o rosto da autora /lesada e o corpo nú de outra mulher. Vide *Acórdão do Supremo Tribunal de Justiça de 21 de Novembro de 2002* (Relator: FERREIRA GIRÃO).

⁹³ Uma providência cautelar que acabaria por ser intentada contra o detentor do *site* obrigou o mesmo a encerrá-lo. Para mais desenvolvimentos vide PAULO BASTOS, “O Direito à Imagem”, *Cyber.net*, n.º 31, pp. 51 a 52 *apud* SOFIA DE VASCONCELOS CASIMIRO, *A Responsabilidade Civil pelo conteúdo da informação transmitida pela Internet*, p. 48, n.75.

tenham decorrido publicamente (v.g. a fotografia das bancadas de um estádio de futebol durante um jogo). Não obstante, se tais retratos, embora aparentemente enquadrados nos casos do n.º2, resultarem no prejuízo para a honra, reputação ou simples decore da pessoa retratada, não poderão ser reproduzidos, nos termos do disposto no n.º3 do artigo 79.º do CC

4.3.2. Violação de direitos de propriedade intelectual

A violação de direitos de propriedade intelectual é comumente aceite como a principal causa da ilicitude de conteúdos colocados e difundidos na Internet. Está na ordem do dia o combate à pirataria, isto é, ao *upload* e *download* de obras protegidas pelo Direito de Autor sem o consentimento do dono da obra. A protecção dos direitos de autor e dos direitos conexos na Internet é, na verdade, a matéria que mais interesse e preocupação tem suscitado na doutrina e jurisprudência, um pouco por todo o mundo, sendo igualmente aquela que mais alterações normativas tem sofrido desde o virar de século, com destaque para as Directivas comunitárias de harmonização de certos aspectos dos direitos de autor e, consequentemente, as alterações às legislações nacionais que essas Directivas têm imposto⁹⁴.

O conteúdo do Direito de Autor, sendo um direito complexo, abrange quer direitos de índole pessoal, ou moral, quer direitos de índole patrimonial. Como direitos pessoais de autor, OLIVEIRA ASCENSÃO⁹⁵ destaca o direito ao inédito, à retirada, ao nome, à paternidade, à integridade e à modificação da obra. Já quanto aos direitos patrimoniais de autor, o ilustre professor distingue entre o direito de participação financeira (direito patrimonial principal) e o direito de sequência, o direito a compensação suplementar por lesão enorme e o direito a compensação devida pela reprodução ou gravação de obras (estes três já direitos patrimoniais que advêm do facto de, devido às condições colectivas de exploração, o anterior direito de exclusivo na exploração da obra ter-se extinguido)^{96 97}.

À primeira vista, poder-se-ia dizer que as violações de direitos de autor existentes na Internet, em particular através de serviços da *web 2.0*, apenas consubstanciam, quase sempre, danos não patrimoniais directos, uma vez que, normalmente, a disponibilização de conteúdos

⁹⁴ Para uma análise das alterações que se têm verificado em matéria de Direito de Autor e direitos conexos *Vide* JOSÉ DE OLIVEIRA ASCENSÃO, “O Direito de Autor e a Internet. Em Particular as Recentes Orientações da Comunidade Europeia”, in *Direito da Sociedade da Informação*, vol. VII, p. 9 ss.

⁹⁵ *Direito Civil: Direito de Autor e Direitos Conexos*, p. 168ss.

⁹⁶ *Idem, Ibidem*, p. 197 ss.

⁹⁷ Não nos cabe aqui entrar em definições do que sejam cada um dos direitos enunciados, tal extravasa o âmbito do nosso estudo. Para mais desenvolvimentos sobre os diferentes direitos abrangidos pelo Direito de Autor, *Vide* OLIVEIRA ASCENSÃO, *Direito Civil: Direito de Autor...*, p. 166ss. e 197ss.

de terceiros não autorizada não é feita com o intuito de explorar economicamente a obra, na medida em que o acesso a tais conteúdos é livre⁹⁸. No entanto, acabarão sempre por existir danos patrimoniais, na medida em que, com a distribuição e reprodução não autorizada das obras protegidas, o autor das mesmas perderá sempre uma quantia monetária pelos utilizadores que adquirem a obra ilegalmente⁹⁹, pelo que o seu direito à participação financeira na obra é afectado¹⁰⁰.

No entanto, hoje em dia, não se pode tomar o Direito de Autor como um direito absoluto, quando confrontado com a liberdade de expressão e de informação que a Internet, em geral, e os serviços da *web 2.0* em particular, proporcionam. A constatação dessa realidade levou à alteração de algumas das noções clássicas do Direito de Autor, como, por exemplo, o direito de reprodução. Mas sobre tais mudanças falaremos mais detalhadamente *infra*¹⁰¹.

4.3.3. Violação de direitos de propriedade industrial

A Internet assume também um espaço por excelência para a perpetuação de violações de direitos de propriedade industrial, em particular atentados contra marcas registadas no mundo analógico.

A este propósito assiste-se ao fenómeno do denominado *cyber-squatting*. O *cyber-squatting* diz respeito a uma técnica que consiste no registo de um “nome de domínio”¹⁰² na Internet, igual ou semelhante ao nome de uma marca do mundo analógico, para posteriormente ser vendida aos titulares da marca a que o nome de domínio faz alusão. Em Portugal, actualmente, não existe qualquer regulamentação específica desta questão e o registo da marca, nos termos do disposto no n.º1 do artigo 224.º do Código da Propriedade Industrial (CPI), apenas confere ao titular da marca o direito de propriedade e do exclusivo da mesma para os produtos e serviços a que esta se destina e dentro de certos limites territoriais –

⁹⁸ Podemos, no entanto, admitir que existe um aproveitamento económico da obra no caso de ela ser disponibilizada numa página *web* que contenha anúncios publicitários que atribuem uma recompensa ao utilizador que gere essa página pelo número de visitantes.

⁹⁹ Caso típico é o da aquisição ilegal de música e filmes.

¹⁰⁰ Sem contar, naturalmente, com as lesões aos direitos secundários do direito patrimonial de autor, como por ex., o direito de sequência.

¹⁰¹ Vide pp. 59 ss.

¹⁰² Por “nome de domínio” entende-se “a porta de entrada para o acesso à informação (página ou sítio) na Internet. Em rigor técnico, o nome de domínio é o conjunto de caracteres – no máximo 63 – que identifica um endereço na rede de computadores Internet (v.g. *www.dominio.pt*).” Noção retirada de JOEL TIMÓTEO RAMOS PEREIRA, *Compêndio jurídico...*, p. 10.

os necessários a não criar confusão no consumidor desses produtos e serviços - não prevendo a sua extensão a nomes de domínio criados com o seu nome.

Não obstante, a jurisprudência portuguesa que se tem pronunciado sobre esta questão, ainda que escassa, tem entendido que a utilização do *cyber-squatting* consubstancia uma prática de concorrência desleal, nos termos do disposto na alínea a) do artigo 317.º do CPI, uma vez que tal acto é susceptível de criar confusão com os produtos e/ou serviços da empresa verdadeiramente titular da marca, independentemente do facto do nome de domínio se encontrar registado em outro país que não o em que foi efectuado o registo da marca.¹⁰³.

4.3.4. Violação do direito de propriedade tout court

Por fim, restará aludir também à possibilidade da lesão à propriedade por força de conteúdos ilícitos colocados e difundidos na Internet. Por exemplo, pense-se na difusão de um vírus na rede, de forma dissimulada, através do envio de mensagens *spam*¹⁰⁴, que, ao ser descarregado, danifica o *hardware*¹⁰⁵ do computador do lesado. Neste caso, existirá uma violação do direito de propriedade do lesado sobre o *hardware* que compõe o seu computador.

As possibilidades de danos causados através da Internet são imensas. Na verdade, à medida que aumentam as suas potencialidades – as quais actualmente se manifestam em grande medida com os serviços da *web 2.0* – também os potenciais riscos se elevam.

¹⁰³ Vide, a título de exemplo, o *Acórdão do Tribunal da Relação de Coimbra de 03 de Junho de 2008* (Relator: BARATEIRO MARTINS), in *Colectânea de Jurisprudência*, 2008, III, p. 22. A Relação entendeu que, apesar do nome de domínio se encontrar registado nos E.U.A., tal produzia efeitos em Portugal, na medida em que os utilizadores da Internet em Portugal poderiam aceder ao site dos E.U.A., produzindo a confusão com os produtos e serviços da empresa titular da marca em Portugal, pelo que se estava perante uma situação de concorrência desleal.

¹⁰⁴ O *spam* representa as mensagens não desejadas que circulam na Internet, nomeadamente através de e-mails de correio electrónico. O nome possui uma origem curiosa, na medida em que advém das latas de carne enlatada de marca SPAM, à venda nos E.U.A. durante o período da II Guerra Mundial. As latas SPAM, embora não fossem do agrado da generalidade dos cidadãos norte-americanos, eram consumidas por obrigação, devido à falta de outros produtos do mesmo tipo, por força do regime de racionamento alimentar em vigor. De igual forma, as mensagens *spam* são mensagens que ninguém quer ler nem as solicitou mas, infelizmente, acabam sempre por aparecer na caixa de correio electrónico. Para mais desenvolvimentos sobre o *spam* vide LUIS MENEZES LEITÃO “A distribuição de mensagens de correio electrónico indesejadas (SPAM)” in *Direito da Sociedade da Informação*, Vol. IV, pp. 191 ss. e, ainda, do mesmo autor, “Comunicações não solicitadas (SPAM)” in *Lei do Comércio Electrónico Anotada*, pp. 213 ss.

¹⁰⁵ Isto é, o conjunto físico dos objectos que compõe um determinado computador.

5. A determinação da culpa do agente na colocação e difusão de conteúdos

5.1. O critério do bonus pater familiae na colocação e difusão de conteúdos online

Um dos critérios fundamentais para a existência de responsabilidade subjectiva é a existência de culpa na actuação do agente, também denominada de nexo de imputação do facto ao agente. A culpa, para que exista, necessita que o agente conheça “ (...) o desvalor da acção que cometeu (ou tivesse podido conhecê-lo), e, bem assim, que tivesse tido a possibilidade de escolher a sua própria conduta (...)” e também que “(...) nas circunstâncias do caso, se possa censurar a conduta levada a cabo pelo agente (...)”¹⁰⁶. A apreciação da culpa é, então assim, feita à luz da diligência de um bom pai de família, em face das circunstâncias de cada caso, nos termos do disposto no n.º2 do artigo 487.º do CC Ou seja, o legislador português, para a determinação da culpa e graduação desta, optou por consagrar o critério tradicional de apreciação da culpa em abstracto, embora não deixe de exigir que tal apreciação tenha em consideração as circunstâncias do caso concreto. Assim, tendo em conta a conduta do homem-médio nas circunstâncias concretas de uma determinada situação em apreço, será possível determinar se o agente agiu ou não com culpa e ainda qual o grau de culpa que lhe pode ser imputável, isto é, saber se o agente agiu a título de dolo ou de mera culpa (negligência)¹⁰⁷.

Na Internet, a colocação de conteúdos ilícitos em rede não importará grandes problemas na determinação da culpa do agente, na medida em que o acto de *upload* de conteúdos ilícitos envolverá necessariamente uma intenção de colocar um determinado conteúdo *online* e uma conformação com o resultado de tal *upload*. O que não significa necessariamente que o agente tenha a intenção de causar um dano a outrem¹⁰⁸. No domínio da Internet, se as ofensas ao bom nome configurarão, na maioria das vezes, situações de dolo directo, já a violação de direitos de autor, será, na maioria das vezes, enquadrável no dolo necessário, uma vez que, como é sabido, a violação destes direitos ocorre, em regra, para evitar o pagamento do preço de venda da obra, sendo a violação do direito uma necessária consequência do acto.

¹⁰⁶ RIBEIRO DE FARIA, *op. cit.*, Vol. I, p. 451.

¹⁰⁷ Embora a imputação da conduta do agente a título de dolo ou de negligência assuma maior importância no campo do Direito Penal, em sede Civil, e mesmo que a actuação dolosa ou negligente conduza em igual medida para a criação da obrigação de indemnizar o lesado, não deixará de ser relevante, nomeadamente na possibilidade de redução equitativa da indemnização nos casos de mera culpa, de acordo com o disposto no artigo 494.º CC

¹⁰⁸ Vide ANTUNES VARELA, *op. cit.*..., p. 593.

No entanto, já no que toca à difusão de conteúdos ilícitos na rede, entendemos que poderão existir alguns problemas adicionais nos casos em que um utilizador ajuda à difusão de um determinado conteúdo pela rede sem intenção dolosa de o fazer¹⁰⁹. Estaremos, *prima facie*, perante casos de mera culpa na difusão de conteúdos ilícitos na Internet. No entanto, a negligência apenas é censurável (e, por conseguinte, leva à responsabilização do agente) quando tal implique a violação de um dever objectivo de cuidado. É, assim, necessário identificar os deveres de cuidado que um utilizador médio deverá observar quando utiliza a Internet, de acordo com o grau de diligência exigido ao *bonus pater familiae*¹¹⁰.

Ora, hoje em dia, perante a democratização da Internet, o utilizador normal da rede não possui especiais conhecimentos de informática. De facto, os serviços disponibilizados *online*, bem como os programas de *software* especialmente criados para uso na rede, actualmente exigem do utilizador apenas uma ligação à Internet. Hoje, o utilizador médio da Internet é um “*leigo em Informática*”¹¹¹. O utilizador não tem, regra geral, qualquer conhecimento especial em tecnologias da informação, nem tão pouco, perante a aparente sensação de segurança na navegação pela Internet, se sente minimamente sensibilizado para a necessidade de instalar programas e mecanismos de defesa contra actuações ilícitas de terceiros, bem como para a adopção de comportamentos de segurança na Internet, como o uso de *passwords* complexas nos serviços que utiliza. Constata-se assim, à primeira vista, a dificuldade em estabelecer padrões mínimos de conduta no uso da Internet a que o utilizador médio deve obedecer para que não seja negligentemente responsável por qualquer conteúdo ilícito difundido através do seu computador e/ou de serviços subscritos por si, como, por exemplo, a sua conta de *e-mail*.

Alguma doutrina tem defendido que, entre os deveres de conduta que o utilizador médio deverá ter de respeitar, está o dever de possuir um programa antivírus¹¹². Não obstante, se o utilizador deve ter um programa antivírus, é imperioso que proceda às suas actualizações, de modo a possuir a versão mais recente sempre que se ligue à Internet. Poderá pôr-se em questão, como faz SOFIA CASIMIRO¹¹³, se ao exigir este tipo de cuidados não se estará a entrar num campo em que os conhecimentos informáticos já não estarão ao alcance do

¹⁰⁹ Veja-se, por exemplo, o caso de um utilizador que, por utilizar uma *password* de acesso à sua conta de *e-mail* pouco individualizada, acaba por permitir que seja apropriada por um *hacker* que, por sua vez, acaba por utilizar a conta para difundir um vírus para a lista de endereços da conta de *e-mail* usurpada.

¹¹⁰ Assim, vide SOFIA CASIMIRO, *op. cit.*, p. 68.

¹¹¹ Expressão emprestada de SOFIA CASIMIRO, *op. cit.*, p. 68.

¹¹² Vide SABRINA MAGNI e MARCO SAVERIO SPLOIDORO, “La Responsabilità degli Operatori in Internet: Profili Interni Internazionali”, in *Diritto dell’Informazione e dell’Informatica*, ano XIII, n.º1, pp.61 ss.

¹¹³ *Op. cit.*, p. 69.

utilizador médio. Refere aquela autora que, a ser assim, “o utilizador médio deverá deter conhecimentos de informática suficientes para evitar a violação, através da Internet, de interesses ou de posições juridicamente protegidas, assim aumentando o grau de diligência exigido ao bom pai de família (...) e assim objectivando, de certo modo, a responsabilidade civil subjectiva”¹¹⁴.

Em nosso entender, a sociedade deverá caminhar no sentido de consciencialização dos utilizadores de Internet, para que estes sejam cada vez mais responsáveis na utilização daquela. Por outro lado, com a evolução dos tempos e da Sociedade da Informação, o utilizador médio será cada vez mais um sujeito que já nasce e cresce rodeado das tecnologias de informação e cujo conhecimento informático será cada vez maior, daí que se deva gradualmente impor ao utilizador médio cada vez mais deveres de cuidado. Sob pena de, caso se proceda em sentido contrário, não poder haver responsabilização do utilizador de Internet senão em casos de dolo.

5.2. Os actos ilícitos cometidos por inimputáveis. A reapreciação da culpa in vigilando

Para que alguém possa ser responsabilizado pelos seus actos é necessário também que seja imputável, isto é, que o agente “ (...) seja capaz de valorar a própria conduta (...) e, do mesmo passo, que se disponha da capacidade necessária para proceder de acordo com a valoração efectuada”¹¹⁵. Por regra, o utilizador da Internet é uma pessoa imputável, isto é, capaz de entender os seus actos e respectivas consequências ou que, pelo menos, devesse conhecer essas consequências. Assim, por exemplo, o utilizador de Internet tem o dever de saber que quando coloca um determinado conteúdo, protegido pelos direitos de autor, num *site* aberto ao público em geral (imaginemos a colocação de parte de um episódio de uma série televisiva no *Youtube*) se encontra a ter um comportamento ilícito (difusão de uma obra sem autorização prévia do seu autor) e não é pelo facto de ser extremamente facilitado o acto de colocação do conteúdo *online* em termos técnicos (exigindo, não raras vezes, apenas dois ou três “cliques”) que o utilizador deixará de poder compreender, ou que lhe será desculpável, o desvalor da sua conduta.

No entanto, apesar da regra, existem sempre excepções. O Código Civil fala, desde logo, em duas excepções, no n.º 2 do seu artigo 488.º: os menores de sete anos e os interditos

¹¹⁴ Idem, p. 70.

¹¹⁵ Vide RIBEIRO DE FARIA, *op. cit.*, p. 452..

por anomalia psíquica. Nestes casos, a Lei civil presume a sua inimputabilidade, ou seja, presume que os sujeitos englobados naquele artigo não têm o discernimento suficiente para entender o desvalor do seu comportamento ou, por outro lado, lhes falta a capacidade de determinar o seu comportamento livremente. Não obstante, no caso em concreto poderá ser afastada a presunção de inimputabilidade que recai sobre aqueles sujeitos, bem como, nos casos em que não haja lugar a presunção de inimputabilidade, poderão os agentes concretos ser considerados inimputáveis.

De todo o modo, caso o agente seja considerado inimputável, em via de regra não será chamado a indemnizar o lesado, salvo em casos excepcionais, como os casos em que não é possível obter a devida reparação das pessoas a quem incumbe a vigilância dos inimputáveis¹¹⁶. Nos casos em que é possível obter a reparação dos vigilantes, são estes os responsáveis, nos termos do disposto no artigo 491.º do CC. É a chamada *culpa in vigilando*.

O artigo 491.º do CC faz presumir a culpa daquele que, por Lei ou por força do negócio jurídico, é obrigado a vigiar outrem, por virtude da incapacidade natural deste. Estas pessoas obrigadas à vigilância de outrem só não serão responsáveis se demonstrarem que cumpriram o seu dever de vigilância ou que os danos se teriam produzido ainda que o tivessem cumprido. Ainda permanecemos no campo da responsabilidade subjectiva, uma vez que a violação do dever de vigilância (embora presumida por Lei) diz respeito a um facto próprio e controlável pela vontade do vigilante¹¹⁷.

No entanto, o disposto no referido artigo 491.º não regula apenas a responsabilidade pelos danos causados por inimputáveis cuja vigilância se encontra a cargo de outrem, mas trata, outrossim, da responsabilidade pelos danos causados por todos os incapazes naturais¹¹⁸. Ou seja, mesmo que o incapaz seja imputável, o seu vigilante continuará a ser responsabilizado (solidariamente com o incapaz, nos termos do disposto no artigo 497.º do CC). Um exemplo deste último tipo de casos prende-se com os menores com mais de sete anos. Continuam a ser incapazes, nos termos dos artigos 122.º e 123.º, ambos do CC, embora, por regra, imputáveis.

Para o que nos interessa, iremos deter-nos no caso dos menores. Como é do senso comum, a facilidade com que a Internet é, hoje em dia, acessível a todos, implica

¹¹⁶ Vide artigo 489.º CC Sobre a temática da inimputabilidade e as hipóteses da sua responsabilização vide, por todos, ANTUNES VARELA, *op. cit.*, pp. 584 ss.

¹¹⁷ Vide ANTUNES VARELA, *op. cit.*, p. 611 ss.

¹¹⁸ Para uma análise detalhada a esta temática vide, por todos, HENRIQUE SOUSA ANTUNES, *Responsabilidade civil dos obrigados à vigilância de pessoa naturalmente incapaz*.

necessariamente que seja utilizada por todos, independentemente da respectiva idade. Por outro lado, as novas gerações tendem a fazer um maior uso das novas tecnologias do que as gerações mais velhas, bem como tendem a “explorar” todas as potencialidades que a *web 2.0* oferece ao utilizador de Internet. Assim, não será incomum encontrar menores que usem e “abusem” da Internet. A questão que se coloca é: nos casos em que um menor coloca ou difunde um conteúdo ilícito em rede, deverão os seus vigilantes (pais e/ou tutores) ser responsabilizados pelos danos que daí ocorram, nos termos da *culpa in vigilando*?

A resposta a esta questão traz-nos alguns problemas, na medida em que, hoje em dia, existem inúmeros locais de acesso à rede, podendo o menor, ainda para mais possuindo um computador portátil, aceder à Internet em praticamente todos os locais que frequenta (pense-se nos inúmeros locais - escolas, cafés, bibliotecas, museus – em que existem redes sem fios - *wireless*), sendo, na prática, impossível que os pais consigam cumprir o seu dever de vigilância. Mesmo em casa, não será, porventura, exigível que os vigilantes do menor monitorizem todas as suas ligações à Internet. De igual forma, à medida que a idade do menor se vai aproximando da maioridade, menor é o conteúdo do dever de vigilância, até porque com o inevitável caminho para a maioridade, os menores precisam “do seu espaço” e o uso da Internet constitui também uma manifestação dessa autonomia crescente. Como salienta HENRIQUE ANTUNES, “O grau de autonomia do filho não se compadece com uma vigilância estrita”¹¹⁹.

O conteúdo do dever de vigilância que impende sobre os responsáveis do menor não é, ainda hoje, questão assente na doutrina e jurisprudência¹²⁰. No entanto, como já anteriormente havíamos defendido¹²¹, entendemos que este dever carece de ser reformulado face à nova realidade digital da Internet. A este respeito, o Acórdão do Supremo Tribunal de Justiça, de 2 de Março de 1978¹²², aponta, em nosso entender, o conteúdo de que se deverá revestir a *culpa in vigilando* na Internet: “ (...) o dever de vigilância deve ser entendido com as circunstâncias de cada caso, não se podendo ser demasiadamente severo a tal respeito, isto porque tanto as concepções dominantes como os costumes influem na maneira de exercer a vigilância de

¹¹⁹ *Idem, Ibidem*, p. 238.

¹²⁰ Assim nos refere MARIA CLARA SOTTOMAYOR, “Responsabilidade civil dos pais pelos factos ilícitos praticados pelos filhos menores”, in *Boletim da Faculdade de Direito*, Vol. LXXI, p. 403.

¹²¹ Vide o nosso “A responsabilidade civil pelo conteúdo da informação...”, p. 11 ss.

¹²² Tal acórdão refere-se a um caso em que um menor de 14 anos matou a tiro outro menor de 13 anos, com uma caçadeira carregada existente em casa dos pais da vítima. O tribunal apurou que o menor não teve culpa uma vez que julgava a arma descarregada. O tribunal decidiu a favor dos réus, afirmando que não haveria previsibilidade da existência da arma num quarto da habitação, pelo que os pais teriam cumprido o dever de vigilância. Vide Acórdão do Supremo Tribunal de Justiça de 2 Março de 1978 in *Boletim do Ministério da Justiça* nº 275, p. 170 ss.

modo a ter de se excluir a culpa de quem, de acordo com aquele costume ou concepção, deixe certa liberdade às pessoas cuja vigilância lhe compete. (...) Os réus (...) não se desleixaram em incutir no filho os princípios de uma boa educação, estimulando-o na prática do bem e reprimindo-o na prática do mal”¹²³.

Julgamos que a consagração, no conteúdo da *culpa in vigilando*, de um critério de *culpa in educando*¹²⁴ é da maior utilidade na nossa problemática, já que o que se deverá exigir dos pais é que eduquem os seus filhos para terem um comportamento “internauticamente” responsável. De facto, se não considerarmos como exigência da *culpa in vigilando*, nesta matéria, uma prova de educação responsável, cairemos em “saco roto”, sob pena da *culpa in vigilando* nunca ser aplicável no domínio da Internet, atentas as impossibilidades fácticas de controlo efectivo dos menores, conforme referido *supra*.

Outro problema também se poderá colocar em relação ao modo de prova de uma *boa educação*. A prova da boa educação não poderá ser demasiado exigente, sob pena de os pais / tutores se verem com o ónus de uma prova diabólica – pois, apesar de tudo, a boa e má educação é algo de muito complexo e subjectivo, sendo difícil de provar diante de um tribunal os conselhos ou exemplos que consubstanciam a educação dada. Deverá assim ser suficiente uma prova genérica de uma boa educação. Prova genérica que não poderá, contudo, deixar de ser valorada sempre com vista ao caso em concreto e nunca em abstracto. Assim, se é certo que, no âmbito da Internet, a prova de uma boa educação passará, nomeadamente, pela demonstração genérica de que os pais tiveram o cuidado de explicar ao filho o que é a Internet e de o acompanhar nas primeiras utilizações da mesma e dos seus serviços, por outro lado, tais deveres de educação já não serão exigíveis a uns pais que nunca a utilizaram (embora estes últimos casos sejam cada vez mais raros no panorama actual).

Não obstante as considerações feitas, admitimos que a *culpa in educando* não possa de imediato ser aplicada no nosso ordenamento enquanto critério autónomo, sem uma intervenção legislativa adequada¹²⁵, não obstante a sua aplicabilidade imediata enquanto critério conformador do conteúdo da *culpa in vigilando*, parecendo ser essa também a

¹²³ *Idem, Ibidem*, p. 172.

¹²⁴ Esta expressão advém do Código Civil Francês de 1804, como nos diz MARIA CLARA SOTTOMAYOR, *op. cit.*, p. 424, n. 76.

¹²⁵ Contra a existência deste critério de *culpa in educando* no nosso ordenamento vide MARIA CLARA SOTTOMAYOR, *op. cit.*, p. 425 ss. Aparentemente a favor da existência de tal culpa no nosso ordenamento vide ADRIANO PAES DA SILVA VAZ SERRA, “Responsabilidade de pessoas obrigadas à vigilância”, in *Boletim do Ministério da Justiça*, nº85, p. 407, bem como HENRIQUE ANTUNES, *op. cit.*, pp. 213 ss.

inclinação da jurisprudência portuguesa¹²⁶. Ao exigir este dever de educação dos menores para as boas práticas em rede estaremos, assim, a admitir ainda a aplicação da *culpa in vigilando* no âmbito de ilícitos praticados na Internet¹²⁷. No fundo, em última análise caberá ao juiz-intérprete, atendendo ao carácter do menor, dos seus pais / tutores e da gravidade do acto ilícito perpetrado na Internet, ajuizar se *in casu* foi cumprido o dever de boa educação. A resposta a tal questão levará o juiz a afastar, ou não, a presunção da *culpa in vigilando*.

5.3. A Internet enquanto excludente da culpa do agente?

Não poderíamos ainda de deixar de analisar a eventual ocorrência de uma causa de exclusão da culpa no que toca aos conteúdos ilícitos colocados e difundidos na Internet. De acordo com PESSOA JORGE¹²⁸ existem três causas de exclusão da culpa: o erro desculpável, o medo invencível e a desculpabilidade. Relativamente ao medo invencível, entendemos que inexistirá qualquer relevância digna de apontamento no que toca a actos ilícitos praticados na Internet, uma vez que tal causa de exclusão da culpa dirá respeito a uma condição – o medo inultrapassável – previamente existente à realidade digital da Internet e, por isso, pertencente ao mundo analógico.

Debatemo-nos, isso sim, pela abordagem ao erro desculpável e à desculpabilidade, devido à natureza da realidade digital da Internet.

Com efeito, a Internet, e em particular a *www*, dá um acesso aparentemente ilimitado ao utilizador, não só para a colocação de conteúdos como para o seu descarregamento. Pode existir, assim, a aparência de que na Internet tudo é permitido e nada é proibido. O utilizador pode representar que, após pagar o acesso à rede (isto é, o pagamento da mensalidade à operadora de telecomunicações para o acesso à Internet) tem direito a usufruir da Internet como bem entender.

Poderemos, pois, estar em face de uma falsa representação da realidade que, face à aparente “liberdade” promovida pela Internet, não pode ser censurada ao agente do facto ilícito – situação de *erro desculpável* – ou, ao invés, não existindo essa falsa representação,

¹²⁶ No *Acórdão de 11 de Julho de 1978*, o Supremo Tribunal de Justiça acabou por condenar os pais de uma criança que feriu outra pelo disparo de uma espingarda de pressão de ar, por *culpa in vigilando* ao não terem instruído devidamente o filho no uso de tal espingarda. *Vide Boletim do Ministério da Justiça*, nº 279, p. 143.

¹²⁷ Distanciamo-nos de SOFIA CASIMIRO, *op. cit.*, p. 72, que entende não restar qualquer espaço para a figura da *culpa in vigilando* no âmbito da actuação na Internet.

¹²⁸ *Apud* MENEZES LEITÃO, *Direito das Obrigações*, p. 329 ss.

atendendo ao meio digital em que se insere a Internet, não era exigível ao agente conduta diversa – situação de *desculpabilidade*.

Em nosso entender, e não obstante considerarmos que a Internet, efectivamente, promove uma aparência de “total licitude” dos conteúdos que nela circulam, temos sérias reservas em admitir a existência destas causas de exclusão da culpa do agente. Desde logo, pelo facto de a actuação ilícita na Internet não ser, do ponto de vista material, diferente da actuação ilícita no mundo real – um acto de difamação feito através de um *post* num determinado *blogue* não é materialmente diverso de um acto de difamação feito através de uma coluna de opinião num determinado jornal impresso – apenas sendo diferente o meio de consumação da violação. Assim, atendendo ao facto de que “*a ignorância da lei não aproveita a ninguém*”, não será devido à aparente facilidade que a Internet propícia quanto à acessibilidade de obtenção ou colocação de conteúdos ilícitos *online* que uma hipotética falsa representação da realidade por parte do agente deixará de lhe ser censurável, ou, por outro lado, não existindo essa falsa representação, que a sua conduta lhe será *desculpável*, uma vez que todo o utilizador tem o dever de saber que “o que é ilícito fora da rede permanece ilícito dentro da rede”¹²⁹.

Assim, a nosso ver, regra geral, tais causas de exclusão da culpa não serão relevantes no que diz respeito à prática de actos ilícitos na Internet.

6. O Dano

6.1. A potenciação do dano na Internet

Por dano considera-se “ (...) toda a perda causada em bens jurídicos, legalmente tutelados, de carácter patrimonial ou não (...)”¹³⁰.

O dano ocorrido no seio da Internet em virtude da colocação de um determinado conteúdo ilícito *online* estará directamente relacionado com a difusão que esse mesmo conteúdo venha a sofrer na rede. O conteúdo tanto poderá ser enviado de um utilizador individual para outro, através de uma mensagem privada de *e-mail* injuriosa, por exemplo, como poderá ser enviado para uma multitude de sujeitos (no caso de, continuando no mesmo exemplo, a mensagem de *e-mail* ser enviada para vários utilizadores), podendo ainda deter um

¹²⁹ Vide *supra*, p. 43

¹³⁰ RIBEIRO DE FARIA, *op. cit.*, p. 480 e 481.

cariz eminentemente público, quando for colocado num *blogue*, rede social ou num outro qualquer *site* de armazenamento de conteúdos aberto à visualização por todo e qualquer internauta.

Assim, no primeiro ou, eventualmente, no segundo grupo de hipóteses mencionadas, a determinação do dano não acarretará grandes dificuldades, uma vez que a difusão do conteúdo se encontra previamente prevista e delimitada, não sendo propriamente diferente, por exemplo, do envio de uma carta injuriosa por via postal. Já no terceiro grupo de hipóteses o dano poderá assumir uma dimensão bastante maior consoante a difusão que o mesmo tiver¹³¹.

Na Internet e, em particular, na *web 2.0*, face à interactividade e partilha de ficheiros entre utilizadores a que a mesma surge associada, a potenciação do dano torna-se uma realidade na medida em que a dimensão dos danos que possam ser suportados por uma determinada esfera jurídica estará sempre dependente da difusão que exista do conteúdo. Isto é, o dano será tanto maior quanto maior for a capacidade de difusão do conteúdo ilícito a partir do local onde este foi colocado¹³².

Pense-se no exemplo do *Facebook*, actualmente a maior rede social do mundo. Um utilizador que contrate os serviços do *Facebook* tem ao seu dispor uma página individual onde pode colocar fotos, vídeos, texto ou qualquer tipo de ficheiro multimédia compatível com a plataforma, bem como efectuar ligações para outros conteúdos existentes em páginas ou *sites* exteriores ao *Facebook*. Qualquer conteúdo que o utilizador coloque na sua página do *Facebook* irá ser visualizada pelos seus “amigos”, os “amigos dos amigos”, ou até o público em geral, consoante as opções de privacidade que o utilizador em questão escolha. Assim, se o conteúdo for ilícito – nomeadamente se consubstanciar uma ofensa ao bom nome ou crédito de outrem – a visualização por todos os sujeitos *supra* referidos irá potenciar manifestamente o dano, bem como a partilha desse mesmo conteúdo pelos restantes utilizadores que o visionem...

Os casos de potenciação do dano serão também existentes nas situações em que sejam colocadas ligações, nomeadamente através de *hyperlinks*, também designadas por ligações de hipertexto¹³³.

¹³¹ Neste sentido *vide* SOFIA CASIMIRO, *op. cit.*, pp. 53 ss.

¹³² Assim, SOFIA CASIMIRO, *op. cit.*, p. 54

¹³³ As ligações de hipertexto possibilitam a mudança directa de uma determinada página onde estão colocadas para outra, no mesmo *site* ou entre *sites* diferentes, através de um simples clique. Podem ser criadas através da marcação de determinadas “palavras-chave” ou da criação de botões próprios cujo clique nas palavras ou botões efectua a mudança pretendida. Os hipertextos podem ser diferenciados entre hipertextos internos ou externos,

Assim, no momento da fixação da indemnização deverão ter-se em consideração todas as manifestações da potenciação do dano, no sentido de atribuir uma maior indemnização ao lesado consoante maior for a referida potenciação, desde que, claro está, tal potenciação ainda seja enquadrável na causalidade adequada do comportamento do agente, sob pena de não se verificar o necessário nexo de causalidade¹³⁴. Ou seja, a potenciação do dano, embora permita o arbitramento de uma indemnização que vá para além do ressarcimento de danos presentes, não poderá servir de alicerce para o ressarcimento de danos futuros ainda não previsíveis, sob pena de violação do disposto no n.º 2 do artigo 564.º do CC

6.2. A reformulação de bens jurídicos alvo de protecção na Internet

A Internet e a *www*, em particular a emergência da chamada *web 2.0*, pelas particularidades que apresentam enquanto meios digitais, admitem novas e inovadoras formas de desempenhar actividades típicas do mundo analógico, de um modo substancialmente diferente do existente fora do mundo digital, o que leva necessariamente a que certos bens jurídicos alvo de protecção pelo Direito e enquadráveis por este no mundo analógico tenham de sofrer alguns desvios para a sua eficaz - e razoável - protecção no mundo digital¹³⁵.

Um particular exemplo desta reformulação de bens jurídicos na Internet - e sobre a qual nos deteremos um pouco - diz respeito à protecção do Direito de Autor na Sociedade da Informação, em particular quanto ao direito de reprodução da obra¹³⁶. Tradicionalmente, a reprodução de uma obra encontrava-se protegida pelo Direito de Autor em todos os casos, apenas podendo ser reproduzida mediante autorização do seu autor. No entanto, a navegação na Internet e o acesso aos seus conteúdos, muitos deles protegidos pelo Direito de Autor, implica a criação de cópias temporárias no computador receptor da informação desses mesmos conteúdos, de modo a serem visualizados pelo utilizador que o pretenda, o que provoca sempre a reprodução da obra. Discutia-se, então, se tais cópias automáticas e transitórias, sem autorização do seu autor, poderiam ou não ser lícitamente utilizadas. A União Europeia, através da Directiva n.º 2001/29/CE, do Parlamento Europeu e do Conselho,

consoante sejam efectuadas para outro local do mesmo *site* ou para outro *site* distinto do primeiro, respectivamente. Para mais desenvolvimentos *vide* MARIO E. CLEMENTE MEORO e SANTIAGO CAVANILLAS MÚGICA, *op. cit.*, pp. 108 ss. e ainda SOFIA CASIMIRO, *op. cit.*, p. 55, nota 93.

¹³⁴ *Vide infra*, pp. 62 ss.

¹³⁵ Já CARNEIRO DA FRADA, ““Vinho novo em odres velhos?...”, pp. 21ss., apontava a necessidade de reformulação dos bens jurídicos objecto de protecção aquiliana na Internet.

¹³⁶ Sobre o direito de reprodução da obra em geral, *vide*, por todos, JOSÉ DE OLIVEIRA ASCENÇÃO, *Direito Civil: Direito de Autor e direitos conexos*, pp. 234 ss.

de 22 de Maio, procurou harmonizar certos aspectos do Direito de Autor e dos direitos conexos na Sociedade da Informação, nomeadamente quanto ao aspecto da reprodução legítima de obras protegidas por aqueles direitos. A Directiva foi transposta no ordenamento jurídico português através da Lei n.º 50/2004, de 24 de Agosto, que procedeu à alteração de vários artigos ao Código de Direitos de Autor e Direitos Conexos (CDADC). Entre essas alterações saliente-se a nova redacção do n.º1 do artigo 75.º do CDADC que exclui do direito de reprodução de obra do autor “(...) os actos de reprodução temporária que sejam transitórios, episódicos ou acessórios, que constituam parte integrante e essencial de um processo tecnológico e cujo único objectivo seja permitir uma transmissão numa rede entre terceiros, por parte de um intermediário, ou uma utilização legítima de uma obra protegida e que não tenham, em si, significado económico (...)”. A norma em destaque permite determinar a licitude das cópias e reproduções automáticas verificadas na Internet, conforme referido, através da exclusão destes actos do direito de reprodução da obra, desde que cumpridos os requisitos enunciados no referido n.º1 do artigo 75.¹³⁷. Assistimos a uma mudança de paradigma quanto ao âmbito de protecção do direito de reprodução da obra.

No entanto, como refere LUÍSA NETO, a Directiva 2001/29/CE, embora tenha modificado em parte o objecto alvo de direitos de autor através da sua abertura às novas tecnologias, não oferece ainda uma regulamentação específica e sistemática para resolver outras novas questões multimédia que se prendem com os direitos de autor na Sociedade da Informação, como sejam a noção de obra, o conteúdo do Direito de Autor, a qualificação dos actos de utilização na Internet, entre outros¹³⁸.

Outro aspecto com relevância, relativamente à reformulação dos bens jurídicos alvo de protecção pelo Direito na Internet, diz respeito ao impacto das ligações de hipertexto sobre os direitos. Relativamente ao Direito de Autor, também foi discutido qual a legalidade do uso de ligações de hipertexto a remeter ou a atribuir acesso a obras protegidas pelo Direito de

¹³⁷ Assim, por exemplo, já será ilícito o *download* de uma obra protegida por direito de autor por parte de um utilizador, uma vez que o *download* implica a criação de uma cópia definitiva e, por isso, não temporária, no disco rígido do computador receptor. Já quanto ao chamado *streaming*, que consiste na visualização de um conteúdo na Internet, utilizando para o efeito a técnica da cópia transitória, subsistem dúvidas quanto à sua licitude ou ilicitude, cuja análise pormenorizada extravasa o âmbito do presente estudo. No entanto, numa primeira análise, somos da opinião que o *streaming* de conteúdos protegidos por direito de autor é ilegal, na medida em que não cumpre o requisito da ausência de significado económico (pense-se, p.e., na visualização de canais de acesso restrito, como a *Sportv*, na Internet, por forma a obstar ao pagamento da mensalidade necessária para a visualização de tal canal).

¹³⁸ Vide, a este respeito, LUÍSA NETO, *Novos Direitos – Ou novo(s) objecto(s) para o Direito?*, pp. 157 ss.

Autor¹³⁹. Hoje é pacificamente aceite que tais ligações são legítimas, correspondendo, grosso modo, a citações, desde que sejam feitas cumprindo os requisitos das mesmas, isto é, não tomando o conteúdo como próprio e indicando devidamente o seu autor.

Questão diversa será a de saber, relativamente a ligações de hipertexto que se façam para outros sites com conteúdos ilícitos, se o utilizador que estabeleça a hiperligação deverá ou não ser responsabilizado pelos danos que daí advierem. De acordo com a dogmática comum da responsabilidade civil, ele seria responsável na medida em que a sua acção desencadeou um dano, ou, pelo menos, potenciou um dano previamente ocorrido. No entanto, em nosso entender, atendendo ao facto de os conteúdos de cada *site* mudarem constantemente, a responsabilidade do utilizador que proceda ao uso de hiperligações não deve ser procedente em todos os casos, na medida em que não será exigível ao utilizador um dever de controlo genérico sobre os conteúdos existentes na totalidade do *site* para o qual a sua hiperligação remete, mas apenas sobre os conteúdos da página do *site* para a qual a hiperligação é feita. Acresce que tal dever de controlo deverá ser avaliado à luz dos conteúdos presentes na página no momento temporal do estabelecimento dessa hiperligação.

Ressalvemos, no entanto, aqueles casos em que o *site* para o qual se remete possui, genericamente conteúdos ilícitos (p.e. um *site* de pedofilia). Neste último tipo de casos, mesmo que a remissão seja feita para uma das páginas do *site* que não possua conteúdos ilícitos, a genérica ilicitude do *site* não pode deixar de ser do conhecimento do utilizador que coloca a remissão e, por isso, deve entender-se que a responsabilidade deste deverá existir, mesmo que o conteúdo ilícito não exista directamente no local para onde a remissão foi feita ou mesmo que os conteúdos ilícitos surjam na página para a qual a hiperligação foi feita em momento posterior à criação desta.

Deste modo, encontramos mais um exemplo onde se deve ponderar a reavaliação do âmbito de protecção pelo Direito de alguns dos bens jurídicos que são susceptíveis de serem violados na Internet.

¹³⁹ Sobre este debate vide PATRICIA AKESTER, *O Direito de Autor e os desafios da tecnologia digital*, pp. 137 ss.

7. O nexo de causalidade entre o dano e o facto ilícito: em especial, a potenciação do dano e a sua imputação ao(s) agente(s)

Aludimos já, em 6.1., ao problema de potenciação do dano a que subjaz a difusão de conteúdos ilícitos na Internet, nomeadamente através do estabelecimento de hiperligações. Agora, analisaremos em que medida a potenciação do dano derivada da sua difusão é susceptível de ser ainda imputável ao primitivo utilizador que o colocou em rede, de acordo com a teoria da causalidade adequada, na sua formulação negativa. É ponto assente que o utilizador primitivo será responsável pelos danos que se revelem condição *sine qua non* da respectiva actuação, num juízo feito quer a nível abstracto quer a nível das circunstâncias em concreto. O nexo de causalidade desempenhará, também na Internet, a sua “ (...) dupla função de pressuposto da responsabilidade civil e de medida da obrigação de indemnizar.”¹⁴⁰.

Em concreto, a verdade é que um conteúdo ilícito colocado em rede constitui condição *sine qua non* dos danos que provoca, independentemente da difusão que sofra. Caso o agente não tivesse colocado o conteúdo ilícito na rede, as difusões do mesmo não existiriam e, por conseguinte, nenhum dano seria causado.

Restará averiguar se tal cenário se mantém num juízo abstracto, isto é, se a previsibilidade da difusão do conteúdo ilícito é legitimamente espectável por parte da generalidade dos utilizadores. Entendemos que sim. Hoje em dia, em pleno zénite da *web 2.0*, os utilizadores, na sua generalidade, têm noção de que os conteúdos que colocam em rede podem ser potencialmente difundidos por outros utilizadores. Assim, consideramos que o utilizador primitivo poderá ser responsabilizado civilmente por todos os danos que advenham, directa ou indirectamente, do seu acto.

Só assim não será se, no caso em concreto, se evidenciarem circunstâncias que possam concluir que não seria previsível tal difusão. Falamos, por exemplo, no caso de o agente divulgar um conteúdo ilícito num fórum de discussão restrito e, posteriormente, um dos seus membros que não o utilizador primitivo difundir o conteúdo para outros locais na rede. Aí, a potenciação do dano já deverá ser ressarcida pelo utilizador que difundiu o conteúdo e não pelo que o colocou, sendo que este apenas será responsável pela sua colocação e pelos danos que aí foram originados.

Mas também poderão ser afastados da responsabilidade do utilizador primitivo casos em que a desproporção entre os danos causados pela colocação do conteúdo e os danos causados

¹⁴⁰ Neste sentido, ALMEIDA COSTA, *op. cit.*, p. 605.

pela sua difusão seja tal que a difusão do conteúdo deixe de ter uma contribuição meramente instrumental ou acessória da causa do dano, para passar a ter uma importância principal. Pense-se, por exemplo, no caso de A colocar uma foto de determinada pessoa, sem o seu consentimento, na sua *homepage*, *homepage* essa que nunca teve muita afluência de visitantes, e a foto é visualizada por B que, por sua vez, resolve colocar uma hiperligação direccionada para a referida foto nas suas cinco *homepages*, todas elas com grande afluência de visitantes. Pense-se ainda que, continuando com o exemplo dado, vários utilizadores criam hiperligações para as *homepages* de B, com o objectivo de divulgarem a foto originariamente colocada por A na sua “incógnita” *homepage*. Nesta situação e em outras semelhantes, a potenciação do dano é de tal forma elevada, em comparação com o dano criado pela colocação do conteúdo, que entendemos não existir nexo de causalidade entre a colocação do conteúdo por A e a potenciação dos danos ocorridos pelas várias hiperligações, criadas por vários e inúmeros utilizadores.

A par da difusão promovida por outros utilizadores também temos a problemática da difusão dada pelos próprios prestadores de serviços intermediários em rede. Como salienta MIGUEL PEGUERA POCH, a verdade é que nenhum dano pode produzir-se na Internet por conteúdos colocados por utilizadores sem o contributo, mesmo que inconsciente, dos prestadores de serviços intermediários que fornecem as ferramentas aos utilizadores para estes colocarem e difundirem conteúdos¹⁴¹. Não obstante, recai sobre estes uma isenção de responsabilidade, desde que os intermediários cumpram determinados requisitos, conforme estudaremos *infra*.

Assim, será sempre necessário fazer-se um juízo em concreto e em abstracto, no sentido de averiguar se a colocação do conteúdo *online* é causalidade suficiente para todos os danos verificados. Caso não seja, e a difusão de conteúdos *online* seja causa determinante dos danos verificados, serão os autores dessa difusão, bem como o agente que colocou os mesmos *online*, responsáveis civilmente pelos danos causados, nos termos do disposto no artigo 490.º CC, sendo que a sua responsabilidade será solidária, nos termos do disposto no artigo 497.º CC, cabendo a cada um direito de regresso face aos demais, em virtude da causalidade de cada actuação para os danos verificados.

¹⁴¹ Vide MIGUEL PEGUERA POCH, *op. cit.*, pp. 29 ss.

8. A actuação do lesado como causa de exclusão ou mitigação da responsabilidade civil na Internet

A própria actuação do lesado pode constituir uma causa de exclusão ou de mitigação da responsabilidade civil em que o agente incorra pelos danos produzidos por um determinado conteúdo ilícito colocado e/ou difundido por aquele na Internet. Por um lado, o seu comportamento, desde que culposos, poderá desencadear uma redução ou até exclusão da indemnização arbitrada, por outro lado, o lesado poderá voluntariamente colocar-se numa situação de perigo, cujos danos daí derivados impeçam o uso do mecanismo da responsabilidade civil.

8.1. A culpa do lesado

Desde logo, a culpa do lesado é, nos termos do artigo 570.º CC, levada em consideração numa eventual indemnização que venha a ser arbitrada por força de um dano produzido por um concreto facto ilícito. A valoração do grau da culpa do lesado na produção do dano será essencial para o julgador manter¹⁴², reduzir ou excluir a indemnização.

No entanto, para que a comparticipação do lesado na produção dos danos seja valorada nos termos *supra* expostos, é necessário que se cumpram determinados requisitos. Desde logo, é necessário que o facto do lesado contribua causalmente para o dano, sendo uma concausa do mesmo, em concorrência com o facto do lesante. Por outro lado, é necessário que o lesado tenha actuado culposamente, isto é, que omita a diligência apta a evitar a produção do dano¹⁴³.

No que toca ao nosso estudo, poder-se-ia, à primeira vista, admitir a aplicabilidade da culpa do lesado às situações em que este omitisse diligências normais de um internauta diligente, como, por exemplo, a utilização de uma *firewall* ou de um *software* anti-vírus durante a navegação na Internet. Caberá diferenciar as situações.

No que respeita à colocação de conteúdos ilícitos na rede, como referimos *supra*¹⁴⁴, tal colocação é sempre premeditada, pelo que o agente age sempre com dolo. Nestes casos, em

¹⁴² Como refere ANTUNES VARELA, *op. cit.*, p. 948, n. 3, “será de manter *toda* a indemnização, quando a culpa do agente seja de tal modo *grave* em confronto com a actuação do lesado, que não justifique a redução dela.” Vide também, a este respeito, *Acórdão do Supremo Tribunal de Justiça de 6 de Julho de 1971*, in *Boletim do Ministério da Justiça*, n.º 209, pp. 102 ss.

¹⁴³ Neste sentido vide RIBEIRO DE FARIA, *op. cit.*, pp. 523 ss.

¹⁴⁴ Vide p. 50

que o agente responsável pelo facto ilícito agiu com dolo, como refere RIBEIRO DE FARIA, deverá ser afastada qualquer relevância da simples culpa do lesado, independentemente da omissão da diligência que lhe seria exigida¹⁴⁵, o que, em nosso entender, também será válido para os danos derivados da colocação de conteúdos ilícitos *online*.

Já no que diz respeito à difusão de conteúdos *online*, se tal difusão for feita a título de negligência, aí a culpa do lesado, *maxime*, a falta de cuidados no sentido de proteger o seu computador contra conteúdos lesivos do respectivo *hardware*, v.g. vírus, conduzirá gradualmente a uma redução da indemnização, na medida em que, à semelhança do que referimos *supra* relativamente à culpa do agente¹⁴⁶, serão gradualmente exigíveis ao utilizador-médio de Internet deveres de cuidado tais como a posse de um *software* de protecção do seu computador e a sua actualização com regularidade. No entanto, terá naturalmente de se ter em conta a capacidade de autodeterminação do lesado, não podendo ser valorada a sua eventual “culpa” na produção do dano se se tratar de um inimputável.

8.2. A autocolocação em perigo. O exemplo paradigmático das redes sociais

Poderá colocar-se em questão se, não se devendo a conduta do lesado a uma omissão da diligência exigida para evitar o dano, poderá na mesma, ser a responsabilidade civil do agente excluída devido ao facto de o lesado, consciente e voluntariamente, se colocar numa situação de perigo.

Estamos a falar da autocolocação em perigo¹⁴⁷. Nestes casos é o lesado que se expõe, de alguma forma, desde que consciente e voluntariamente, a um determinado risco, a uma situação de perigo. É, por isso, essencial, para a operação do instituto, que o lesado preveja, mesmo que numa percentagem reduzida, a possibilidade do risco / perigo ocorrer.

No âmbito da Internet, assume particular interesse averiguar em que medida a utilização de redes sociais, nomeadamente o *Facebook*, entre outras, poderá consubstanciar uma autocolocação em perigo. Isto porque os serviços de redes sociais disponíveis permitem geralmente ao utilizador que estipule as suas próprias definições de privacidade, nomeadamente quanto às pessoas a que torna acessível o seu perfil na rede social. Poder-se-á colocar em questão saber se um determinado utilizador que, ao permitir que o seu perfil seja

¹⁴⁵ *Op. cit.*, p. 524.

¹⁴⁶ *Vide* pp. 51 ss.

¹⁴⁷ Também apelidado de “assunção do risco”. A este respeito *vide* JOSÉ CARLOS BRANDÃO PROENÇA, *A conduta do lesado como pressuposto e critério de imputação do dano extracontratual*, pp. 620 ss.

acedido por qualquer outro utilizador da rede social em causa, coloca fotos reveladoras da sua vida privada, poderá depois vir pedir uma hipotética indemnização ao prestador do serviço pelo facto de a sua página de perfil ter sido divulgada por inúmeros utilizadores da rede social, consubstanciando uma violação do seu direito à reserva da intimidade da vida privada.

Pensamos que não. Com efeito, neste caso, o lesado assumiu com o seu comportamento (colocar a sua página de perfil disponível para todos os restantes utilizadores e divulgar fotos da sua vida privada aos mesmos) o risco inerente à utilização das redes sociais sem qualquer “filtro” de privacidade, que é precisamente o da divulgação, sem limites, do seu perfil. Assim, não terá este lesado direito a qualquer indemnização por se ter conformado com o risco existente. No entanto, será sempre necessário, como referimos, que o risco se encontre inerente ao comportamento manifestado e seja previsível pelo lesado¹⁴⁸. Caso, p. e., em virtude do comportamento *supra* referido, o utilizador se visse inundado de comentários injuriosos à sua pessoa, aí já não se poderia falar em autocolocação em perigo, na medida em que o risco associado ao seu comportamento não comportava a previsão de danos ao bom nome do utilizador em causa.

De igual forma poderá existir autocolocação em perigo por parte do lesado se este utiliza a Internet para aceder a conteúdos ilícitos (p. e. a obras “pirateadas”) e ao pensar que se encontra a descarregar um determinado conteúdo, acaba por, sem o saber, descarregar um vírus para o seu computador. Embora a intenção do lesado não fosse descarregar o vírus mas sim o conteúdo (ainda que ilícito), o lesado, atendendo ao conhecimento da ilicitude do conteúdo que se encontrava a transferir, não poderia deixar de prever como possível que tal conteúdo fosse, na verdade, um vírus. O risco, o perigo, encontrava-se assim, dentro da esfera de previsibilidade do lesado, atendendo ao comportamento consciente e voluntariamente adoptado.

9. O problema do anonimato na Internet

9.1. O anonimato enquanto corolário do direito à reserva da intimidade da vida privada

“*On the internet, nobody knows you’re a dog*”¹⁴⁹, expressão utilizada por PETER STEINER, numa famosa vinheta de banda desenhada publicada na edição de 5 de Julho de

¹⁴⁸ Esse juízo de previsibilidade far-se-á, também, tendo por padrão o homem-médio.

¹⁴⁹ “Na internet ninguém sabe que és um cão”. Tradução livre nossa.

1993 do jornal *New Yorker*¹⁵⁰, bem ilustra o anonimato subjacente à navegação na Internet pela grande maioria dos utilizadores. Por anonimato entendemos, claro está, a não identificabilidade da pessoa física do utilizador que acede à Internet.

No entanto, ao contrário do que à primeira vista poderia parecer, o anonimato é, via de regra, lícito, enquanto manifestação ou corolário do direito à reserva da intimidade da vida privada, protegido constitucionalmente nos termos do disposto no artigo 26.º da Constituição da República Portuguesa.

O utilizador, na *www*, local onde é constantemente observado, tem direito a poder proteger determinadas informações pessoais que não pretenda divulgar, de modo a evitar que possam colocar em perigo a sua segurança e/ou provocar prejuízos inevitáveis ao seu bom nome ou reputação¹⁵¹.

No entanto, constata-se que na *www* o direito ao anonimato é constantemente violado, através da colocação dos designados *cookies*¹⁵² nas várias páginas a que o utilizador acede quando navega na Internet.

O anonimato constitui, como dissemos, corolário do direito à reserva da intimidade da vida privada. Desde que utilizado, como também referimos, de forma legítima. Ou seja, já não encontrará protecção constitucional o uso do anonimato com o objectivo de cometer actos ilícitos na rede.

Deste modo, caso um utilizador anónimo cometa um acto ilícito na rede, as autoridades competentes terão legitimidade para solicitar junto dos prestadores de serviços intermediários desse utilizador, os dados pessoais do mesmo, com vista à sua identificação, para ser sujeito a responsabilidade civil e/ou criminal¹⁵³. O RJCE prevê na alínea b) do seu artigo 13.º, a obrigação de os prestadores intermediários de serviços identificarem os destinatários dos serviços com quem tenham acordos de armazenagem face a pedido da entidade competente. O Decreto-lei não estipula em que situações o pedido ou a satisfação do mesmo deve ser cumprido, mas, em nosso entender, de acordo com o *supra* exposto, apenas será legítimo à entidade competente solicitar tais informações quando tiver fundadas suspeitas de que o utilizador em causa praticou um acto ilícito, sob pena de violação do direito ao anonimato.

¹⁵⁰ *Apud* CHRIS REED, *op. cit.*, p. 140.

¹⁵¹ Assim, JOEL TIMÓTEO RAMOS PEREIRA, *Direito da Internet e Comércio Electrónico*, p. 20 e *Compêndio jurídico...*, p. 21.

¹⁵² Sobre a noção de *cookie* vide *supra*, p. 45, n. 87

¹⁵³ Não descaramos de observar, contudo, que a maior parte dos intermediários não terá informações verdadeiras sobre o utilizador, na medida em que a maior parte dos contratos de prestação de serviços na *web 2.0*, como já referimos, é feita a título gratuito, o que leva à falta de interesse dos intermediários em obter informações fidedignas.

9.2. Formas de que se pode revestir o anonimato

Desde logo, o anonimato na Internet é manifestado pelo facto da identificação *online* ser efectuada pelo IP – *Internet Protocol* que, como referido *supra*¹⁵⁴, identifica apenas o computador que emite os dados para serem transportados na rede, não possibilitando determinar em concreto a pessoa que se encontra a aceder à Internet com aquele computador em específico. Como aponta CHRIS REED, “(...) a identificação digital de um utilizador não tem necessariamente uma ligação com a sua identificação no mundo analógico”¹⁵⁵.

Se o computador pessoal de um determinado sujeito, via de regra, é utilizado no acesso à *www* por esse mesmo sujeito, o mesmo não sucede em inúmeros outros casos em que, por exemplo, o acesso à Internet é feito através de um ciber-café, através de computadores existentes numa biblioteca ou universidade, entre outros. E, mesmo em agregados familiares, onde a ligação de Internet é efectuada por um único terminal de acesso, torna-se bastante difícil descortinar qual a pessoa do agregado que utilizou o acesso à Internet para fins ilegítimos.

Esta será, porventura, a manifestação analógica do anonimato na Internet, mas, em pleno ambiente digital, também existem várias formas de evitar que o IP de um determinado computador seja conhecido, nomeadamente através de técnicas de *spoofing*. O *spoofing* consiste na apropriação de determinados elementos informáticos alheios, com o intuito de evitar a localização real do computador. Geralmente, o *spoofing* é desencadeado mediante o registo de um nome de domínio muito semelhante ao de um *site* pré-existente, de modo a que um determinado utilizador, por inadvertência ou erro, passe a navegar nesse novo *site* criado para o *spoofing*. O utilizador, ao navegar nesse *site* falso, encontra-se a fornecer à pessoa que criou o *site* elementos pessoais, como, para o que nos interessa, o endereço de IP. Posteriormente, no que é apelidado de *IP spoofing*, é alterado o IP de origem do sujeito que pratica o *spoofing*, mantendo, na aparência, a mesma sequência numérica do IP terceiro que foi apropriado, de forma a poder ser utilizado para entrar em servidores restritos (por exemplo, o uso de um IP alheio para entrar num serviço contratado por este e cuja permissão para aceder se faz por reconhecimento de IP) ou, então, para praticar actos ilícitos, colocando as “culpas” em terceiros¹⁵⁶.

¹⁵⁴ Vide nota 6, p. 20

¹⁵⁵ *Op. cit.*, p. 140 (tradução livre nossa).

¹⁵⁶ Para mais desenvolvimentos vide JOEL TIMÓTEO RAMOS PEREIRA, *Compêndio jurídico...*, pp. 465 ss.

O *spoofing*, além de ser uma técnica absolutamente ilegal em si mesma, por violar grosseiramente dados pessoais de um determinado internauta, permite a prática de qualquer acto ilícito na Internet sem possibilidade de identificação do verdadeiro agente.

Outra técnica vulgarmente utilizada para a prática de actos anónimos é a do envio de mensagens de correio electrónico anónimas, denominadas de *anonymous remailers*, que consistem no envio de mensagens de correio electrónico com a possibilidade de colocação de uma identidade falsa do remetente da mensagem (isto é, um endereço de e-mail que não corresponde ao real), bem como no envio de mensagens sem qualquer identificação do remetente¹⁵⁷.

9.3. Conclusão: a impraticabilidade da responsabilidade civil dos autores do acto ilícito

Por não ser possível associar o IP a um determinado sujeito em particular, mas apenas ao computador do qual provém o acto ilícito, bem como, pelos mecanismos que existem para ocultar o verdadeiro IP, teremos forçosamente de concluir pela impraticabilidade da responsabilidade civil dos autores do acto ilícito, por via de regra¹⁵⁸.

O problema principal reside no facto de ser impossível, pelo menos na actual configuração abrangente do direito à reserva da intimidade da vida privada, proibir o uso do anonimato *tout court* e, por essa via, não ser exigível aos vários intervenientes na Internet que se assegurem que os sujeitos com quem interagem na rede são efectivamente quem dizem ser. Como salienta GIUSEPPE CASSANO, “(...) o problema da responsabilidade civil na Internet continua a ser o centro de um grande dilema para os governos dos vários Estados e as organizações jurídicas internacionais. Por um lado, a possibilidade de conservar o anonimato

¹⁵⁷ Vide, entre outros, SOFIA CASIMIRO, *op. cit.*, pp. 77 ss. e LUCIA MARÍN PEIDRO, *op. cit.*, pp. 78 ss.

¹⁵⁸ Poder-se-ia colocar em questão a responsabilidade civil do dono da coisa, *in casu*, do proprietário do computador utilizado para o acesso à Internet e, conseqüentemente, para a colocação de conteúdos ilícitos em rede. No entanto, tal hipótese torna-se impraticável se tivermos em conta que uma das técnicas de *IP spoofing* a que aludimos *supra* permite o acesso de um determinado computador à Internet utilizando o IP de outro. Assim, além da indeterminabilidade do sujeito que acedeu à Internet também nos deparamos em grande parte dos casos com a indeterminabilidade da máquina que foi utilizada para o acesso à Internet. Além do mais, pense-se na existência de vários computadores em Escolas, Bibliotecas e até *ciber-cafés* e depressa se concluirá também pela impraticabilidade de imposição de uma responsabilidade sobre o dono da coisa, sob pena do proprietário ser obrigado a impor uma série de filtros e condicionamentos aos utilizadores desses computadores que depressa retirariam qualquer utilidade no seu uso. Não obstante, a Lei HADOPI, à qual faremos referência no capítulo IV do nosso estudo – Vide pp. 129 ss. – impõe ao titular da conta de acesso à internet, que é, a maioria das vezes, também o proprietário do computador utilizado nesse mesmo acesso, o ónus de provar que o acto ilícito não foi praticado por si. Sobre a bondade desta solução nos pronunciaremos também no referido capítulo.

é essencial para a manutenção, no ciberespaço, do direito à reserva da intimidade da vida privada e liberdade de expressão. Por outro lado, a possibilidade de participar e comunicar na rede, sem necessidade de revelar a própria identidade, pode revelar-se contrária (...) às iniciativas governamentais de combate os conteúdos ilícitos na Internet (...)”¹⁵⁹.

Perante estes dois opostos, é necessário encontrar um ponto de equilíbrio. Já o referimos: apenas poderá ser permitida a utilização do anonimato para fins lícitos. Caso seja utilizado para fins ilícitos, então as autoridades judiciais competentes terão legitimidade para exigir dos prestadores de serviços intermediários a identificação dos seus clientes.

Não obstante, na falta de identificação dos utilizadores infractores, o que sucederá, como vimos, na maior parte das vezes, torna-se necessário, de modo a evitar a completa inutilidade do instituto da responsabilidade civil na Internet, procurar outros sujeitos identificáveis que tenham também, de algum modo, contribuído, mesmo que inconscientemente, para os danos.

Neste quadro, é equacionada a responsabilidade civil dos prestadores de serviços intermediários em rede, encontrando-se hoje, na ordem do dia, determinar se o regime vigente da sua responsabilização é, ou não, suficiente para a efectivação prática da responsabilidade civil na Internet. Será essa análise que iremos fazer, nos próximos dois capítulos deste estudo.

¹⁵⁹ *Op. cit.*, p. 341. Tradução livre nossa.

CAPÍTULO III

A RESPONSABILIDADE CIVIL DOS PRESTADORES DE SERVIÇOS INTERMEDIÁRIOS NA REDE

10. Evolução histórica da responsabilização dos prestadores de serviços intermediários

Desde cedo se procurou imputar os danos ocorridos em esferas jurídicas alheias através de actos ilícitos praticados na Internet aos prestadores de serviços intermediários na rede. Na verdade, este foi um dos primeiros problemas jurídicos a surgir no âmbito da Internet¹⁶⁰.

A tentativa de responsabilização dos prestadores de serviços ocorre por duas ordens de razões: a primeira proporcionada pela extrema dificuldade, já constatada¹⁶¹, de identificação do infractor, ao contrário do que sucede com os prestadores de serviços intermediários, na medida em que estes, tratando-se, na sua generalidade, de sociedades comerciais registadas, são facilmente localizáveis e identificáveis¹⁶²; a segunda devido a uma maior solvabilidade financeira dos prestadores intermediários de serviços em comparação com os utilizadores causadores dos danos, o que, permite, naturalmente, um ressarcimento integral do dano do lesado.

No entanto, sempre se debateu (e ainda se debate) em que moldes poderia um prestador de serviços intermediários na Internet ser responsabilizado por conteúdos colocados por terceiros. Este debate foi, e é, protagonizado por dois grupos de interesses diametralmente opostos: de um lado, os próprios prestadores de serviços intermediários na Internet que sempre advogaram, em defesa da sua “irresponsabilidade”, a sua qualidade de meros “mensageiros” e, ainda, a impossibilidade técnica do controlo dos conteúdos, colocados por terceiros, que transmitem e alojam nos seus servidores e os elevados custos financeiros que tal obrigação de controle, a ser imposta, acarretaria para a sua actividade, o que iria obstar

¹⁶⁰ Quem o diz é LILIAN EDWARDS, “The Fall and Rise of Intermediary Liability Online” in *Law and the Internet*, p. 48.

¹⁶¹ Vide *supra* pp. 69 ss.

¹⁶² Refira-se que, embora a DCE imponha, no seu artigo 4.º, o princípio da não sujeição da actividade do prestador de serviços em rede a autorização prévia dos Estados membros, nada obsta a que os Estados Membros imponham uma “obrigação de inscrição” dos prestadores de serviços junto das entidades responsáveis quando estes pretendam exercer a sua actividade estabelecidos num determinado Estado, como uma forma de auxílio à mais rápida identificação do prestador e da obtenção de informações ou imposição de deveres sobre o mesmo. É o que sucede no ordenamento jurídico português, que determina, nos termos do disposto no n.º 4 do artigo 4.º do RJCE que “Os prestadores intermediários de serviços em rede que pretendam exercer estavelmente a actividade em Portugal devem previamente proceder à inscrição junto da entidade de supervisão central.”

irremediavelmente ao desenvolvimento do comércio electrónico e à expansão da Internet, bem como colidir ou restringir o direito à liberdade de expressão de cada utilizador em livremente publicar os seus conteúdos na rede¹⁶³; do outro lado, os lesados, *maxime*, as associações de gestão colectiva dos direitos de autor e direitos conexos, que, perante a impossibilidade prática de ressarcimento dos danos pelos autores materiais do ilícito, invocam a obrigatoriedade dos intermediários controlarem previamente os conteúdos que permitem que sejam colocados e difundidos através das próprias tecnologias que eles mesmos colocam à disposição dos utilizadores e, conseqüentemente, a sua responsabilização pela falta de incumprimento desta obrigação, sob pena de falhar qualquer possibilidade real de impedir a propagação de conteúdos ilícitos através da Internet.

Até ao início do século XXI, na ausência de um critério uniforme nos diversos ordenamentos jurídicos, as decisões jurisprudenciais foram diversas, assentando também em critérios distintos, pendendo para cada “lado da balança” conforme as circunstâncias.

Iremos agora analisar, brevemente, a evolução jurisprudencial e legislativa ocorrida quer nos E.U.A., quer na União Europeia.

10.1 Estados Unidos da América

Um dos primeiros casos jurisprudenciais de relevo ocorreu nos E.U.A., em 1991. Tratou-se de um litígio que opôs uma sociedade comercial, a *Cubby Inc.*, e o *Compuserve Inc.*, um dos primeiros prestadores de serviços intermediários *online*¹⁶⁴. Em resumo, a *Cubby* procurou responsabilizar a *Compuserve* por esta alojar um jornal electrónico onde tinha sido colocada uma mensagem que ofendia o bom nome da *Cubby*. O tribunal absolveu a *Compuserve* entendendo que esta não poderia ser considerada uma editora dos conteúdos que eram armazenados no seu servidor, na medida em que, na sua actividade de alojamento de conteúdos nos seus servidores, a *Compuserve* não tinha nenhuma interferência directa nos mesmos, sendo apenas um mero “distribuidor”. O tribunal entendeu de igual forma que não seria razoável impor à *Compuserve* uma obrigação de prévio exame e análise de cada mensagem armazenada nos seus servidores, perante a constatação da impossibilidade técnica do prestador cumprir essa eventual obrigação.

¹⁶³ Vide, a este respeito, a interessante comunicação de CYNTHIA WONG, do Centro para a Democracia & Tecnologia, intitulado *Intermediary Liability: protecting internet platforms for expression and innovation*.

¹⁶⁴ *Cubby Inc. v. Compuserve Inc.* (1991). Sobre este caso, vide, entre outros, SOFIA CASIMIRO, *op. cit.*, p. 83 ss.

Porém, em sentido contrário pronunciou-se a jurisprudência norte-americana, no caso *Playboy v. Frena*¹⁶⁵, que entendeu responsabilizar o intermediário *Frena*, por alojar no seu *site* imagens protegidas pelos direitos de autor da empresa *Playboy* que tinham sido colocadas por um utilizador cuja identificação não foi possível obter.

Em 1995, o tribunal da Califórnia acabou por ditar a sentença que marcou a tendência seguida pela jurisprudência norte-americana. No caso *Religious Technology Center v. Netcom Online Communications Services Inc.*, discutia-se se o *Netcom*, um prestador de serviços intermediários *online*, podia ser responsabilizado pela violação de direitos de autor do fundador da Igreja de Cientologia, por parte de um utilizador dos serviços que o próprio intermediário disponibilizava. Neste caso foram demandados o utilizador e o prestador intermediário, o *Netcom*, este último com base na sua passividade, por não ter removido o conteúdo ilícito, não obstante o pedido da Igreja de Cientologia feito à *Netcom* nesse sentido. A *Netcom*, por sua vez, defendeu-se referindo que não tinha possibilidades técnicas para localizar o conteúdo ilícito e, por outro lado, que a demandante não tinha demonstrado que os conteúdos colocados estavam efectivamente protegidos pelo Direito de Autor. O tribunal da Califórnia acabou por absolver a *Netcom* do pedido, referindo, nas suas conclusões, que: o intermediário de serviços em rede não podia ser responsável directo pelo acto ilícito, na medida em que o conteúdo ilícito tinha sido fornecido por um seu utilizador; também não podia ser responsabilizado a título subsidiário uma vez que não existia ligação entre os benefícios económicos da actividade do intermediário e as actividades ilícitas levadas a cabo pelos seus utilizadores; por fim, inexistia também uma responsabilidade concorrente, na medida a *Netcom* não tinha incentivado a conduta ilícita do utilizador¹⁶⁶.

Assim, nos E.U.A., passou a existir uma tendência generalizada de aplicação do princípio da não responsabilização dos prestadores intermediários de serviços. O precedente nos tribunais estadunidenses era que não se poderia exigir dos intermediários um dever geral de controlo do conteúdo da informação transmitida. Tal posição alicerçava-se, no nosso entender, em duas razões de fundo: por um lado, na importância destacada da liberdade de expressão¹⁶⁷ – e que corria o risco de ser limitado pela imposição de um “controle prévio” dos conteúdos colocados em rede por parte dos intermediários responsáveis pelo seu transporte

¹⁶⁵ *Playboy Enterprises Inc. v. Frena* (1993). Vide, por todos, LUCIA MARÍN PEIDRO, *op. cit.*, p. 85 e 86.

¹⁶⁶ *Religious Technology Center v. Netcom Online Communications Services Inc.* (1995). Vide LUCIA MARÍN PEIDRO, *op. cit.*, p. 87 e 88.

¹⁶⁷ Que constitui a Primeira Emenda à Constituição Norte-Americana e que, por conseguinte, possui geral prevalência sobre a maioria dos restantes direitos fundamentais, ao contrário do que sucede, por exemplo, no ordenamento jurídico português.

e/ou alojamento – como elemento essencial à expansão da Internet; por outro lado, na falta de possibilidades técnicas de exercer o referido “controlo prévio” dos conteúdos sem comprometer inevitavelmente as principais vantagens da utilização da Internet – extrema rapidez no acesso e na transmissão de conteúdos.

Esta tendência foi acolhida na secção 230 do *Communications Decency Act*, de 1996, que garante a todos os prestadores de serviços intermediários *online* imunidade contra qualquer acção judicial que vise responsabilizá-los por conteúdos gerados por terceiros, no que respeita a conteúdos difamatórios ou violadores da reserva da intimidade da vida privada (designada nos E.U.A. por *privacy*). Esta foi também a primeira intervenção legislativa no sentido de regulação do conteúdo da informação transmitida pela Internet¹⁶⁸.

O *Communications Decency Act* previa uma imunidade total para os intermediários, mesmo que estes tivessem conhecimento do conteúdo ilícito e nada fizessem para o retirar¹⁶⁹. Resultava, por isso, que o Senado Norte-Americano tinha privilegiado absolutamente a eficiência do comércio electrónico e a expansão da utilização da Internet, em prejuízo da tutela dos lesados. No entanto, a referida lei apenas era aplicável aos casos de ofensas ao bom nome e à reserva da intimidade da vida privada.

De modo algo diferente entendeu o Senado quando votou favoravelmente a aprovação do *Digital Millenium Copyright Act* (DMCA), em 14 de Maio de 1998, destinado a regulamentar a utilização de obras protegidas pelo Direito de Autor (*Copyright*) através de sistemas informáticos. O DMCA, embora prevendo, por regra, a “irresponsabilidade” dos intermediários de serviços em rede, instituía várias obrigações que os prestadores intermediários tinham de cumprir para beneficiarem da referida isenção de responsabilidade.

Desde logo, o DMCA, enquanto regime opcional e voluntário para os intermediários *online*¹⁷⁰, impõe três obrigações gerais para que estes possam beneficiar do seu regime: que os intermediários informem os seus clientes - utilizadores das condições de rescisão do contrato de prestação de serviço, bem como dos pressupostos que darão lugar à mesma; que os

¹⁶⁸ Disso nos dá conta SOFIA CASIMIRO, *op. cit.*, p. 111. Para um enquadramento geral sobre o *Communications Decency Act* a respeito da difamação *vide*, por todos, RUTH HILL BRO, “Defamation Online”, in *Online Law*, pp. 335 ss.

¹⁶⁹ Não obstante, a referida lei previa a responsabilização dos intermediários relativamente à difusão de conteúdos considerados obscenos ou indecentes que fossem inapropriados a menores de 18 anos. No entanto, esta disposição foi julgada inconstitucional pelo Supremo Tribunal dos Estados Unidos, por violar a liberdade de expressão, consagrada na Primeira Emenda à Constituição. Para mais desenvolvimentos *vide* SOFIA CASIMIRO, *op. cit.*, p. 112 ss.

¹⁷⁰ Os prestadores de serviços intermediários poderiam optar por não ser abrangidos pelas disposições do DMCA, no entanto, ficariam abrangidos pelo regime geral do *copyright* norte-americano que não possuía isenções de responsabilidade, sendo, por isso, um regime totalmente desfavorável quando comparado com o DMCA.

intermediários não interfiram nos conteúdos dos seus utilizadores¹⁷¹, designadamente permitindo o uso das tecnologias necessárias para que estes possam proteger as suas obras; por fim, que os intermediários protejam a intimidade e privacidade dos seus utilizadores, não ficando, assim, sujeitos a uma obrigação de controlo dos conteúdos que são colocados e difundidos pelos seus sistemas tecnológicos¹⁷².

De seguida, o DMCA diferencia vários regimes de “isenção de responsabilidade” consoante a actividade que o prestador leve a cabo. Caso a actividade do prestador consista no mero transporte de conteúdos, este não será responsabilizado, desde que não tenha interferência directa nos referidos conteúdos (isto é, que não os seleccione, nem os modifique, etc...). Se essa atitude consistir no armazenamento temporário de conteúdos (o já referido *caching*¹⁷³), o intermediário não será responsável desde que o alojamento temporário tenha como objectivo uma transmissão mais rápida e eficiente dos conteúdos. Se, porventura, consistir no armazenamento principal, o intermediário não será responsável se cumprir três requisitos: não ter conhecimento próprio do carácter ilícito do conteúdo; não receber um benefício económico directamente relacionado com o conteúdo ilícito; por fim, retirar ou impossibilitar o acesso, com celeridade, ao conteúdo ilícito, logo que seja notificado por um interessado da existência do mesmo¹⁷⁴. Caso os intermediários levem a cabo actividades de associação de conteúdos (isto é, disponibilização de motores de busca para pesquisa de diversas informações), estes não serão responsáveis desde que cumpram os requisitos referidos para os serviços de armazenamento principal da informação.

Em resumo, podemos concluir que, no que toca ao Direito estadunidense, este sempre demonstrou uma tendência “desresponsabilizante” dos prestadores de serviços intermediários em rede, tendência essa que foi pautada pelo valor primordial que a liberdade de expressão representa no ordenamento jurídico norte-americano, bem como na expansão da Internet como corolário consequente daquele valor.

¹⁷¹ Salvo nos casos em que os conteúdos sejam ilícitos, como veremos *infra*, pp. 84 ss.

¹⁷² Vide LUCIA PEIDRO, *op. cit.*, p. 88 ss.

¹⁷³ Vide *supra*, p. 34.

¹⁷⁴ O chamado mecanismo *notice and take-down*, apelidado assim no direito anglo-saxónico.

10.2 União Europeia

Nos Estados-Membros da União Europeia, curiosamente, a tendência observada até ao início do século XXI foi precisamente em sentido contrário à verificada nos E.U.A.: responsabilização dos prestadores intermediários de serviços pelos conteúdos ilícitos colocados por utilizadores.

O Reino Unido, em 1998, deparou-se com o primeiro processo judicial que trouxe o debate sobre a responsabilidade dos prestadores de serviços intermediários *online* para as ilhas britânicas. No processo *Godfrey v. Demon Internet*, o Dr. Lawrence Godfrey, professor de física, processou o intermediário *Demon Internet* por este armazenar nos seus servidores um grupo de discussão onde tinha sido colocada uma mensagem difamatória do Dr. Godfrey. O Dr. Godfrey enviou uma carta à *Demon*, solicitando que esta procedesse à eliminação da mensagem, no entanto, o intermediário, apesar de ter os meios técnicos para tal, nada fez, tendo a mensagem vindo a ser eliminada automaticamente dez dias após a sua colocação no grupo de discussão. A *Demon* deduziu a sua defesa ao abrigo do *Defamation Act* britânico, de 1996, alegando que se limitava a ser a proprietária dos servidores onde as mensagens eram armazenadas e uma mera distribuidora dessas mensagens, não podendo tais serviços ser equiparados a serviços de publicação. Não obstante, o tribunal, numa decisão preliminar do processo, afasta a defesa deduzida pela *Demon*, qualificando os serviços desta como serviços de publicação – salientando, inclusive, que a razão de ser de um entendimento diverso do observado pela generalidade da jurisprudência norte-americana se prendia justamente com a diferença entre o valor atribuído à liberdade de expressão neste ordenamento (valor constitucional primordial) e no ordenamento britânico, que conduzia a entendimentos diversos no que tocava à matéria da difamação¹⁷⁵. Atenta esta decisão preliminar, as partes chegaram, posteriormente, a acordo, uma vez que seria quase certa a condenação da *Demon* caso o processo seguisse para julgamento.

Em França, grande parte da jurisprudência foi no sentido da responsabilização dos intermediários, impondo em vários casos uma responsabilidade por culpa presumida e impondo deveres aos intermediários que quase implicavam uma responsabilidade objectiva dos mesmos. A título de exemplo, refira-se o caso de 1998, que opôs *Estelle Hallyday*, uma conhecida modelo francesa, e *Altern Org.*, um fornecedor de alojamento, por este albergar, no

¹⁷⁵ *Godfrey v. Demon Internet* (1998). Para mais desenvolvimentos sobre a responsabilidade dos intermediários por actos difamatórios no ordenamento jurídico britânico vide CHRIS REED, *op. cit.*, pp. 112 ss. e GRAHAM J. H. SMITH, *Internet Law and Regulation*, pp. 81 ss.

seu servidor, páginas electrónicas onde foram colocadas, por um utilizador anónimo, fotografias da autora nua, sem que esta tivesse consentido na divulgação das mesmas. O *Cour d'Appel* de Paris, chamado a pronunciar-se sobre esta questão, decidiu que, para que o intermediário se pudesse eximir da responsabilidade, deveria provar que tinha cumprido com a obrigação de informar o utilizador em questão das normas de respeito pelos direitos de personalidade. De igual forma considerou que o intermediário tinha a obrigação de supervisionar os conteúdos alojados no seu servidor, considerando, para todos os efeitos, que este tinha um papel igual ao de um editor¹⁷⁶.

Esta decisão foi severamente criticada pelas associações dos intermediários de serviços *online*, bem como pelas associações defensoras da liberdade de expressão. Os primeiros alegavam que decisões como a verificada em Paris implicariam demasiados custos que acabariam, no curto-médio prazo, por eliminar os pequenos prestadores de serviços intermediários do mercado. Já os segundos referiam que uma imposição, aos intermediários, de deveres genéricos de controlo sobre os conteúdos levaria a que estes se convertessem em censores, limitando-se assim, irremediavelmente, a liberdade de expressão permitida pela rede.

Em Itália, até ao surgimento da DCE, a responsabilização dos intermediários era feita com base nos preceitos gerais do *Codice Civile*. A jurisprudência italiana pronunciava-se no sentido da responsabilidade do intermediário, na medida em que este, como transmissor do conteúdo ilícito, desenvolvia uma conduta causal e adequada à produção do dano, ao mesmo tempo que alguma doutrina estudava vias de responsabilização objectiva dos intermediários pelos conteúdos colocados e difundidos através dos seus servidores¹⁷⁷.

Na Alemanha, a tendência inicial fora também no sentido de responsabilizar os intermediários de serviços. Tal aconteceu com o caso *Compuserve*, em 1995, em que a filial alemã da prestadora de serviços intermediários norte-americana foi processada por permitir o acesso a vários grupos de notícias (*newsgroups*) que difundiam mensagens de pornografia infantil ilícitas. A *Compuserve* foi responsabilizada pelo facto de o tribunal de primeira instância considerar que a actuação do intermediário não seria diferente da de um editor e, por isso, impedia sobre o mesmo o dever de controlo dos conteúdos aos quais permitia o acesso. No entanto, esta decisão veio a ser revogada em sede de recurso, entendendo o tribunal *ad quem* que na altura em que ocorreram os factos inexistia tecnologia suficientemente eficaz

¹⁷⁶ *Estelle Haliday v. Altern Org.* (1998).

¹⁷⁷ Para uma análise mais detalhada ao regime jurídico italiano anterior à DCE *vide*, entre outros, GIUSSEPPE CASSANO, *op. cit.*, em especial pp. 342 ss.

que permitisse à *Compuserve* bloquear os conteúdos em causa e, por isso, nunca a sua actividade poderia ser comparada à de um editor, uma vez que este, pela sua própria natureza, tem um efectivo poder de controlo sobre o(s) conteúdo(s) que se publica(m)¹⁷⁸.

O caminho europeu distanciou-se assim do caminho norte-americano. Todavia, atentas as decisões jurisprudenciais tomadas em desfavor dos intermediários e as consequências negativas que tal acarretaria para o comércio electrónico e a expansão da Internet em geral¹⁷⁹, alguns dos Estados da Europa procuraram regular a questão, indo no sentido do “princípio da irresponsabilização” dos intermediários. Tal sucedeu nos ordenamentos francês e alemão, com a publicação da *Loi Relative à la Liberté de Communication*, de 1996, e da *Informations- und Kommunikationsdienste Gesetz* (a chamada Lei Multimédia), de 1997, respectivamente. Ambas as leis dispunham no sentido da responsabilização dos intermediários de serviços *online* por conteúdos colocados em rede por terceiros apenas e unicamente quando aqueles desempenhassem actividades de armazenamento de conteúdos, tivessem conhecimento dos conteúdos ilícitos e nada o fizessem para os remover. Nos restantes casos apenas seriam responsabilizados se tivessem contribuído directamente para a criação ou produção dos conteúdos ilícitos.

Nesta perspectiva, o Parlamento Europeu e o Conselho, atentas as necessidades de incrementar e desenvolver o comércio electrónico e, também, a harmonização legal e jurisprudencial entre os Estados-Membros e entre estes e países terceiros (nomeadamente os E.U.A.), resolveram aprovar a Directiva n.º 31/2000/CE, vulgarmente designada por Directiva do comércio electrónico (DCE). A DCE, além de regular vários aspectos do comércio electrónico, procurou regulamentar a responsabilidade dos prestadores de serviços intermediários em rede, no sentido de limitar a sua responsabilidade a casos estritos e impor a ausência de uma “obrigação geral de vigilância” sobre os conteúdos de terceiros transmitidos pelos intermediários, obrigação essa que teria de ser cumprida por todos os Estados-Membros, quer na transposição da DCE, quer na regulamentação de outros aspectos do comércio electrónico que a Directiva deixasse ao dispor de cada Estado. Acolheu, assim, como

¹⁷⁸ Para uma análise da evolução histórica da corrente jurisprudencial e legal alemã, relativa à responsabilidade dos prestadores de serviço intermediários na Internet *vide*, por todos, THOMAS HOEREN, “Liability for online services in Germany”, in *German Law Journal*, vol. 10, n.º 5, pp. 561 ss.

¹⁷⁹ Veja-se, a título de exemplo, que a decisão judicial relativa ao processo *Godfrey v. Demon Internet* teve como reflexo, nos anos seguintes, o aumento da recusa de manutenção de alojamento de páginas electrónicas por parte dos intermediários nos casos em que existia algum risco de o conteúdo das mesmas ser considerado difamatório. Neste sentido veja-se SOFIA CASIMIRO, *op. cit.*, pp. 90 ss.

principais fontes inspiradoras quer a a DMCA norte-americana, quer a Lei Multimédia alemã, *supra* referidas¹⁸⁰.

Em suma, a União Europeia aproximou-se do regime norte-americano. Privilegia-se, actualmente, a limitação da responsabilidade dos intermediários de serviços, em detrimento da tutela dos potenciais lesados pelos conteúdos que circulem em rede¹⁸¹.

10.3 O panorama português

Em Portugal, um pouco devido à escassez de prestadores de serviços intermediários sedeados no país, bem como ao facto de, na maior parte dos litígios existentes, as partes chegarem a acordo, ou se tratar de casos em que o utilizador que comete o acto ilícito é conhecido (o que não comporta problemas de maior), o desenvolvimento jurisprudencial desta temática tem sido quase inexistente¹⁸².

Não obstante, desde cedo que a doutrina portuguesa se tem pronunciado no sentido da não imposição aos intermediários do dever geral de vigilância dos conteúdos por eles transmitidos, contando que o façam de forma automática e sem conhecimento da sua ilicitude¹⁸³.

Essa posição acabou por ser, em menor ou maior medida, a seguida pela DCE e, posteriormente, transposta para o nosso ordenamento jurídico através do Decreto-Lei n.º 7/2004, de 7 de Janeiro, alterado pelo Decreto-Lei n.º 62/2009, de 10 de Março, que vimos a

¹⁸⁰ Vide pp. 72 ss.

¹⁸¹ Outros ordenamentos jurídicos procuraram, também, impor aos prestadores intermediários de serviços uma responsabilidade objectiva, ou pelo risco. A este respeito refira-se a decisão do *Tribunal da Cámara Civil y Comercial* da província de Jujuy, na Argentina (Processo nº B-85235/02) onde existiu a condenação do proprietário de um fórum de discussão (cuja função desempenhada se assemelha em muito ao dos intermediários de armazenamento principal), por conteúdos ilícitos aí colocados por terceiros. Na fundamentação, o tribunal invocou a responsabilidade objectiva do proprietário, associando a actividade da Internet a uma actividade perigosa, de grande risco, como sucede com quem detém uma instalação de electricidade ou gás, aplicando analogicamente um artigo em tudo semelhante ao nosso artigo 509.º CC Tal situação, em nossa opinião, carece de qualquer fundamento. A Internet, por demais riscos que possa encerrar em si, nunca deverá ser entendida como actividade perigosa. Ela é uma manifestação da liberdade de informação e de expressão e, como tal, está sujeita a limites que têm de ser descortinados *in casu*. A este respeito vide JOEL TIMÓTEO RAMOS, *Compêndio jurídico...*, p. 876ss.

¹⁸² Ressalvam-se algumas providências cautelares que têm sido intentadas, como sucedeu com o conhecido *site* “Fototanga”.

¹⁸³ Neste sentido, veja-se o estudo pioneiro de CARNEIRO DA FRADA, ““Vinho novo em odres velhos?....”

designar como Regime Jurídico do comércio electrónico (RJCE)¹⁸⁴ e cuja análise faremos de seguida.

11. O panorama vigente: o Regime Jurídico do Comércio Electrónico

Conforme referido *supra*, o Decreto-Lei n.º 7/2004, de 7 de Janeiro, alterado pelo Decreto-Lei n.º 62/2009, de 10 de Março, transpõe para a ordem jurídica nacional a Directiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de Junho de 2000 (DCE), instituindo assim o RJCE. Vejamos os traços mais importantes do diploma, no que toca à responsabilidade civil dos prestadores de serviços intermediários em rede:

11.1 Âmbito de aplicação

O RJCE aplica-se a qualquer “serviço da sociedade da informação”, definindo como tal “ (...) qualquer serviço prestado à distância por via electrónica, mediante remuneração ou pelo menos no âmbito de uma actividade económica na sequência de pedido individual do destinatário.”¹⁸⁵. Esta definição é, por isso, crucial para a determinação do âmbito de aplicação do diploma. Para que o serviço prestado seja considerado “serviço da sociedade da informação” e, conseqüentemente, esteja dentro do âmbito de aplicação do RJCE, é necessário que: a actividade seja prestada à distância; com recurso à via electrónica; mediante a existência de um pedido individual do destinatário; por fim, que seja um serviço prestado mediante remuneração, ou, pelo menos, no âmbito de uma actividade económica^{186 187}.

Não obstante o *supra* exposto, o RJCE não se aplicará a “serviços da sociedade da informação” que contendam com as seguintes matérias: matéria fiscal; disciplina da concorrência; regime do tratamento de dados pessoais e da protecção da privacidade; patrocínio judiciário; jogos de fortuna, incluindo lotarias e apostas, em que é feita uma aposta em dinheiro; actividade notarial ou equiparadas, enquanto caracterizadas pela fé pública ou por outras manifestações de poderes públicos¹⁸⁸.

¹⁸⁴ O referido Decreto-Lei tem sido também apelidado de Lei do Comércio Electrónico. Não obstante se tratar de um mero “preciosismo”, entendemos, por uma questão de correcção formal, uma vez que o regime foi aprovado por Decreto-Lei, tomar a designação dada em texto.

¹⁸⁵ Cfr. artigo 3.º, n.º1, do RJCE.

¹⁸⁶ O que engloba também, como já referido *supra*, os serviços prestados aos utilizadores de forma gratuita, embora com o intuito de obtenção de lucro por outras vias, como anúncios publicitários.

¹⁸⁷ Neste sentido veja-se CLÁUDIA TRABUCO, *op. cit.*, pp. 475 ss.

¹⁸⁸ Cfr. artigo 2.º, n.º1, do RJCE.

11.2. Princípio da equiparação

O artigo 11.º do RJCE estipula que “A responsabilidade dos prestadores de serviços em rede está sujeito ao regime comum (...) com as especificações constantes dos artigos seguintes.”. Assim, é claro que o RJCE não pretende criar um regime autónomo de responsabilidade dos prestadores de serviços intermediários em rede, mas, ao invés, “filtrar” as circunstâncias concretas em que os intermediários, cumpridos que estejam determinados requisitos (previstos nos artigos 13.º ss. do RJCE), se encontram “isentos de toda a responsabilidade”¹⁸⁹. A regra continua a ser o princípio de responsabilidade, no sentido de imputação dos danos a uma esfera jurídica distinta daquela em que os mesmos se repercutiram, reunidos que estejam os respectivos pressupostos, embora, em termos práticos, como veremos *infra*, difícil será a não sujeição da actividade concreta do intermediário aos requisitos de “isenção” da responsabilidade.

De todo o modo, fruto deste princípio da equiparação, caso a actuação do intermediário de serviços não seja subsumida a alguma das condições de isenção de responsabilidade tal não implica necessariamente que o mesmo seja automaticamente responsabilizado. É necessário ainda que se cumpram os cinco requisitos da responsabilidade civil¹⁹⁰, apesar de, no nosso entender, como veremos *infra*¹⁹¹, a não subsunção a algumas das condições de isenção de responsabilidade implicar a verificação automática do preenchimento de algum ou alguns dos requisitos de responsabilidade civil¹⁹².

11.3. Ausência de um dever geral de vigilância

O artigo 12.º do RJCE é o reflexo da imposição da DCE aos Estados-Membros, no sentido de estes não exigirem dos prestadores intermediários de serviços uma obrigação geral de vigilância sobre os conteúdos colocados por terceiros que circulem nos seus servidores¹⁹³.

¹⁸⁹ Embora, como refere PEDRO ROMANO MARTINEZ, “Responsabilidade dos prestadores de serviços em rede”, in *Lei do Comércio Electrónico Anotada*, p. 269, não se deva levar à letra a expressão “isento de toda a responsabilidade”. O intermediário “estará isento de toda a responsabilidade se, dentro do panorama comum e relacionado com as regras gerais se puder concluir nesse sentido”.

¹⁹⁰ Vide MIGUEL PEGUERA POCH, *op. cit.*, pp. 35 ss.

¹⁹¹ Vide pp. 91 ss.

¹⁹² Neste sentido vide SANTIAGO CAVANILLAS MÚGICA, “ Responsabilidad civil” in *Deberes y responsabilidades de los servidores de acceso y alojamiento: un análisis multidisciplinar*, p. 51, n. 3.

¹⁹³ Cfr. artigo 15.º, n.º1 da DCE.

Nos termos do normativo nacional, “Os prestadores intermediários de serviços em rede não estão sujeitos a uma obrigação geral de vigilância sobre as informações que transmitem ou armazenam ou de investigação de eventuais ilícitos praticados no seu âmbito.” No entanto, como refere CLÁUDIA TRABUCO, cuja posição subscrevemos, “não obstante o estabelecimento deste princípio básico, *prima facie* contrário à responsabilização dos prestadores de serviços, não deve retirar-se desta regra uma total ausência de obrigações pendentes sobre estes nos casos de violações cometidas por terceiros com utilização dos seus serviços”¹⁹⁴.

Assim, independentemente da subsunção da sua conduta aos requisitos excludentes da sua responsabilidade, impendem sobre os prestadores intermediários de serviços várias obrigações, desde logo as previstas no artigo 13.º do RJCE. Dizem respeito aos deveres comuns que os prestadores intermediários de serviços devem observar para com as entidades competentes, como sejam as de informar as mesmas logo que tenham conhecimento de actividades ilícitas que se desenvolvam por via dos serviços que prestam, satisfazer os pedidos de identificação dos destinatários dos serviços com quem tenham acordos de armazenagem, cumprir prontamente as determinações destinadas a prevenir ou pôr termo a uma infracção e fornecer listas de titulares de *sites* que alberguem, quando lhes for pedido.

A par das referidas obrigações genéricas, ainda podem impender sobre os prestadores intermediários de serviços outras obrigações consoante o tipo de serviço que prestem (v.g. *infra* quanto aos serviços de armazenagem principal). Ponto em aberto é se, para além das obrigações presentes no referido regime, podem ser impostas aos prestadores intermediários outras obrigações *ex novo* e se tal imposição conflituará com a norma do artigo 12.º.

A este respeito, no chamado “Caso *Promusicae*”, em Espanha, a propósito de uma petição que a sociedade gestora de direitos de autor *Promusicae* lançou sobre a operadora de telecomunicações *Telefónica* para que esta revelasse a identificação dos utilizadores que fizessem *downloads* ilegais de música, o próprio Tribunal de Justiça das Comunidades Europeias (actual Tribunal de Justiça da União Europeia) veio reafirmar que as directivas europeias para a Sociedade da Informação (entre elas, a DCE) não impõem aos Estados-Membros a previsão da obrigação de divulgar os dados pessoais dos utilizadores de Internet aos prestadores de serviços, sendo que na transposição das directivas e na sua execução se deve procurar uma interpretação do Direito Estadual conforme ao Direito Comunitário, de

¹⁹⁴*Op. cit.*, p. 486.

modo a assegurar um “justo equilíbrio” entre os direitos e os princípios comunitários (entre eles o princípio da proporcionalidade)¹⁹⁵.

11.4. A responsabilidade em caso de simples transporte ou fornecimento de acesso

Dispõe o artigo 14.º do RJCE que “o prestador intermediário de serviços que prossiga apenas a actividade de transmissão de informações em rede, ou de facultar o acesso a uma rede de comunicações, sem estar na origem da transmissão nem ter intervenção no conteúdo das mensagens transmitidas nem na selecção destas ou dos destinatários, é isento de toda a responsabilidade pelas informações transmitidas.”

Trata-se de uma isenção de carácter objectivo, na medida em que o legislador exceptiona de qualquer tipo de responsabilidade a actividade levada a cabo pelo intermediário (dentro de determinados parâmetros), independentemente da actuação do mesmo¹⁹⁶.

Assim, para que o fornecedor de *mero transporte* de informações¹⁹⁷ ou de *fornecimento de acesso* à rede não esteja abrangido pelo regime geral da responsabilidade civil torna-se necessário que não esteja na origem da transmissão do conteúdo e não tenha intervenção no conteúdo das mensagens nem na selecção destas ou dos seus destinatários.

Compreende-se que assim seja. A prestação da actividade de simples transporte ou acesso à rede é eminentemente técnica e automatizada, de natureza passiva, o que implica, naturalmente, que o prestador intermediário não tem conhecimento da informação transmitida ou armazenada, nem o controlo da mesma¹⁹⁸.

Naturalmente, se o prestador de serviço estiver na origem da transmissão do conteúdo ilícito ou tiver intervenção no conteúdo das mensagens, na selecção das mesmas ou dos seus destinatários, será responsável, nos termos gerais, conforme dispõe o já citado artigo 11.º do RJCE, na medida em que, nestes casos, não se encontram reunidas as características da automaticidade e passividade na transmissão e/ou acesso à informação.

Poder-se-á colocar a questão de saber se a colocação de filtros automáticos nos dispositivos de transmissão de informações, por parte destes intermediários, constitui uma

¹⁹⁵ Acórdão do Tribunal de Justiça das Comunidade Europeias n.º C-275/06, in *Jornal Oficial da União Europeia*, 8.3.2008, p. C64/10.

¹⁹⁶ Vide MIGUEL PEGUERA POCH, *op. cit.*, p. 36. A posição legislativa adoptada pelo legislador comunitário relativamente aos prestadores de serviços de *mero transporte ou acesso à rede* coloca-nos, no entanto, algumas reservas, como veremos *infra*, pp. 102 ss.

¹⁹⁷ Ou, em linguagem anglo-saxónica, *mere conduit*.

¹⁹⁸ Assim se referiram o Parlamento Europeu e o Conselho no considerando n.º 42 da DCE.

selecção de mensagens nos termos e para os efeitos do artigo 14.º do RJCE e, por conseguinte, exclui a actividade do prestador do regime de isenção da responsabilidade.

No nosso entender, a colocação de tais filtros, desde que seja efectuada com carácter automático e isento (isto é, cujas finalidades sejam a melhoria das condições do serviço prestado, nomeadamente com vista à eliminação de mensagens não solicitadas, também conhecidas por *spam*), não configura uma selecção das mensagens a transmitir, para efeitos do disposto no artigo 14.º. Isto porque o artigo 14.º pretende excluir da isenção de responsabilidade as actuações quase-autorais do intermediário (casos em que ele próprio origina a transmissão ou altera as informações transmitidas) bem como a colaboração no acesso, mais fácil ou mais dirigido, a conteúdos ilícitos¹⁹⁹. Ora, a colocação de filtros automáticos não se enquadra nem na primeira nem na segunda das hipóteses referidas²⁰⁰.

11.5. A responsabilidade em caso de armazenagem

Nos termos do disposto nos artigos 15.º e 16.º do RJCE, o intermediário que proceda à prestação de serviços de armazenagem fica isento de responsabilidade desde que observe determinada conduta, isto é, desde que cumpra vários deveres que lhe são impostos. Trata-se, assim, ao contrário do que sucede com a isenção prevista no artigo 14.º do RJCE, de uma isenção de carácter subjectivo, na medida em que faz depender a aplicação do regime da isenção do cumprimento de certos níveis de diligência por parte do intermediário²⁰¹.

Como já referido, a armazenagem pode ser temporária ou principal. Consoante o tipo de armazenagem que o prestador de serviços intermediários leve a cabo na sua actividade, será sujeito a diversos deveres de conduta, conforme veremos *infra*.

a) Armazenagem temporária

A armazenagem temporária encontra-se prevista no artigo 15.º do RJCE²⁰². O normativo dispõe quer obrigações de carácter negativo quer obrigações de carácter positivo, que

¹⁹⁹ Neste sentido, SANTIAGO CAVANILLAS MÚGICA, *op. cit.*, pp. 50 ss. Porém, no sentido de admitir uma possível responsabilidade pela colocação deste tipo de filtros vide JOEL TIMÓTEO RAMOS PEREIRA, *Compêndio...*, pp. 875 ss.

²⁰⁰ Claro está que a colocação de filtros de modo a que apenas sejam transmitidas mensagens de determinado teor já não configura um carácter isento, pelo que, nestes casos, se as mensagens transmitidas forem ilícitas, o intermediário já será responsável.

²⁰¹ Vide MIGUEL PEGUERA POCH, *op. cit.*, p. 36.

²⁰² Não podemos deixar de lamentar o facto de, na transposição da directiva, o legislador português ter optado por trocar a designação da directiva – “armazenagem temporária” – por outra – “armazenagem intermediária” –

impendem sobre o intermediário de modo a que este se encontre isento de toda e qualquer responsabilidade.

Desde logo, tal como sucede com o mero transporte ou acesso, o intermediário é obrigado a abster-se de comportamentos que extravasem a dita actividade de armazenagem temporária (ou *caching*), isto é, a armazenagem tem de ser efectuada com o único e exclusivo propósito de tornar mais eficaz a transmissão posterior da informação, a nova solicitação do destinatário²⁰³. Para tal, é essencial, conforme refere CLÁUDIA TRABUCO²⁰⁴, que o intermediário: não modifique a informação; respeite as condições de acesso à mesma e as regras relativas à actualização da informação²⁰⁵, indicadas de forma amplamente reconhecida e utilizada pelo sector; por fim, que não interfira com a utilização legítima da tecnologia, aproveitando-a para obter dados sobre a utilização da informação.

O artigo 15.º do RJCE ainda estabelece, no seu n.º 3, uma obrigação positiva de não armazenamento dos materiais que deixem de estar disponíveis na fonte originária, seja porque os mesmos foram retirados pelo próprio fornecedor dos mesmos, seja porque foi ordenada a sua remoção por um tribunal ou entidade administrativa competente, seja porque o acesso a esses materiais foi tornado impossível. Da letra da lei parece resultar que a obrigação de retirada destes materiais da memória *cache* existe quer o material seja ou não ilícito, ficando o prestador sujeito ao regime geral da responsabilidade civil caso não retire o material *tout court*. Naturalmente, o prestador apenas será responsabilizado se o material em causa for considerado ilícito e desde que se cumpram os restantes requisitos da responsabilidade civil.

b) Armazenagem principal

A armazenagem principal encontra-se consagrada no artigo 16.º do RJCE²⁰⁶ e, apesar de ter um conteúdo semelhante à armazenagem temporária, os deveres que impendem sobre o intermediário que proceda à armazenagem principal são mais exigentes do que aqueles que impendem sobre o intermediário que proceda à armazenagem temporária.

quando, na realidade, uma vez que estamos a falar de prestação de serviços intermediário, qualquer uma das actividades de armazenagem – temporária ou principal – será sempre intermediária, pelo que não foi feliz o legislador nesta alteração.

²⁰³ Cfr. n.º 1 do artigo 15.º do RJCE.

²⁰⁴ *Op. cit.*, p. 489.

²⁰⁵ O que necessariamente leva a concluir que o prestador será responsável se não proceder à sistemática actualização da informação armazenada.

²⁰⁶ Na transposição do artigo 14.º da DCE – correspondente ao aqui analisado artigo 16.º do RJCE – o legislador nacional foi mais feliz na alteração da designação “armazenagem em servidor”, constante da Directiva, para “armazenagem principal”, uma vez que a primeira designação poderia levar a enganos na determinação do âmbito de aplicação da norma, na medida em que a armazenagem, temporária ou principal, será sempre efectuada num servidor.

Compreende-se que assim seja, já que o artigo 16.º (e o correspondente artigo 14.º da DCE) se reporta, fundamentalmente, às actividades de *hosting*, isto é, de alojamento de conteúdos a pedido de um determinado utilizador para ser visualizado e/ou descarregado por outros. É também este, com maior ou menor complexidade, o serviço intermediário tipicamente utilizado para a colocação de conteúdos gerados pelos utilizadores²⁰⁷.

Desde logo, a isenção de responsabilidade é afastada quando o destinatário do serviço actua subordinado ao intermediário ou é por este controlado, nos termos do disposto no n.º 3 do artigo 16.º. Esta norma pretende afastar o regime de isenção aos casos em que exista uma relação de comissão entre o destinatário do serviço e o intermediário. A *ratio* da norma pretende excluir da isenção a responsabilidade por conteúdos que sejam colocados por quem tenha uma estreita conexão com o intermediário de serviços, uma vez que, por um lado, não existe a distância necessária entre o conteúdo ilícito e o intermediário que possa justificar um alegado estado de “desconhecimento” da existência do conteúdo e, por outro lado, o intermediário possui possibilidade de actuar sobre para justificar a isenção²⁰⁸.

Nos termos do disposto no n.º 1 do artigo 16.º do RJCE, o intermediário será isento de toda a responsabilidade pelos conteúdos ilícitos armazenados no seu servidor se não tiver conhecimento da actividade ou informação cuja ilicitude seja manifesta ou, tendo conhecimento, não retirar ou impossibilitar logo o acesso a essa informação²⁰⁹.

O intermediário de armazenamento principal será ainda responsável civilmente se, nos termos e para os efeitos do disposto no n.º 2 do artigo 16.º do RJCE, tiver ou dever ter consciência do carácter ilícito da informação. Note-se que, apesar de o normativo não o referir, apenas relevará para efeitos de aplicabilidade do n.º 2, que a ilicitude da informação seja manifesta, na medida em que todo o escopo normativo do artigo 16.º foi construído tendo por base a ideia de “ilicitude manifesta”²¹⁰.

Uma última nota, que se prende com uma inovação do legislador nacional, face ao legislador comunitário: é prevista, no n.º 6 do artigo 18.º do RJCE, a isenção de

²⁰⁷ MIGUEL PEGUERA POCH, *op. cit.*, pp. 45 ss., referindo-se ao teor do artigo 14.º da DCE alerta para a falta de precisão da norma, na medida em que a mesma, da forma como está redigida, pode acabar por ser aplicável a uma variedade de situações, algumas das quais poderão não ter sido previstas pelo legislador comunitário. A título de exemplo, veja-se que esta norma, pela sua abrangência, será aplicável ao armazenamento de páginas pessoais, blogues, perfis em redes sociais, caixas de correio electrónico, entre muitos outros.

²⁰⁸ Neste sentido *vide* CLÁUDIA TRABUCO, *op. cit.*, p. 490 e ainda JOSÉ DE OLIVEIRA ASCENÇÃO, *Bases para uma transposição da directriz n.º 00/31, de 8 de Junho (Comércio Electrónico)*, Apud *Lei do Comércio Electrónico Anotada*, p. 61.

²⁰⁹ *Vide* CLÁUDIA TRABUCO, *op. cit.*, p. 490.

²¹⁰ O que é, aliás, corroborado no artigo 18.º do RJCE, referente à solução provisória de litígios, quando no seu n.º 1 refere que “Nos casos contemplados nos artigos 16.º e 17.º, o prestador intermediário de serviços, se a ilicitude não for manifesta, não é obrigado a remover o conteúdo contestado (...)”.

responsabilidade do intermediário face a um utilizador que tenha colocado um determinado conteúdo *online* e que seja entretanto removido pelo intermediário, desde que tal remoção tenha sido derivada de uma solicitação prévia de um alegado interessado e a falta de ilicitude do conteúdo não seja manifesta. Tal isenção já se encontrava prevista no DMCA, no entanto, o legislador comunitário, na DCE, optou por não a incluir, o que poderá levar a que o intermediário, face a esta falta de isenção, tarde na resposta a uma qualquer reclamação, com vista a não retirar conteúdos não ilícitos, o que poderá levar a uma ainda maior potenciação do dano do lesado. Com a solução legal do n.º6 do artigo 18.º, a posição do lesado é acautelada, assim como a do intermediário, na remoção de conteúdos²¹¹.

11.6. A associação de conteúdos

A problemática da associação de conteúdos foi deixada de fora da DCE, muito embora tal não tenha obstado a que alguns dos Estados-Membros tivessem optado por regular esta matéria por si mesmos, tal como sucedeu em Portugal²¹².

Importará, em primeiro lugar caracterizar a actividade da associação de conteúdos. A actividade de associação de conteúdos não consubstancia, em nosso entender, uma actividade diferente das restantes actividades de intermediação que expusemos *supra*²¹³, mas, ao invés, uma mitigação entre a actividade de armazenamento e a actividade de acesso. Armazenamento, pois a associação de conteúdos consiste no alojamento de hiperligações para variadíssimos *sites*. Acesso, pois o clique nessas hiperligações permite ao utilizador ter acesso aos *sites* para os quais aquelas remetem²¹⁴.

O artigo 17.º do RJCE equipara a responsabilidade dos prestadores de serviços intermediários de associação de conteúdos à responsabilidade dos prestadores de serviços intermediários de armazenagem principal.

Não obstante, o RJCE, no seu artigo 19.º, faz referência à actividade de associação de conteúdos em geral, dispondo o seu n.º1 que “A associação de conteúdos não é considerada irregular unicamente por haver conteúdos ilícitos no sítio de destino, ainda que o prestador tenha consciência do facto.” O disposto no normativo acabado de referir parece entrar em

²¹¹ O que não evita, claro está, uma desvantagem para a posição do utilizador que coloca o conteúdo *online*, *maxime*, para a liberdade de expressão, como veremos *infra*, pp. 104 ss.

²¹² Sendo que também Espanha e Áustria procederam a essa regulamentação.

²¹³ Vide pp. 32 ss.

²¹⁴ Como exemplos de serviços de associação de conteúdos podemos indicar os motores de pesquisa, sendo os mais conhecidos o motor de busca da *Google* e o *Bing*, motor de busca da *Microsoft*.

conflito com o disposto no artigo 17.º, na medida em que, de acordo com este último, se o prestador de serviços intermediários de associação de conteúdos tiver conhecimento do conteúdo ilícito deverá impossibilitar desde logo o acesso a tal conteúdo²¹⁵.

De acordo com o Gabinete de Política Legislativa e Planeamento do Ministério da Justiça²¹⁶, a maneira como as duas normas são formuladas aponta, no entanto, para uma contrariedade apenas aparente. Na verdade, o disposto no artigo 17.º consagra, por remissão para o disposto no artigo 16.º, um dever de o prestador de serviços intermediários de associação de conteúdos impossibilitar o acesso a tal conteúdo mal tenha conhecimento, por intermédio próprio ou de outra pessoa, da ilicitude do conteúdo para o qual o serviço remete. Por outro lado, o artigo 19.º parece aplicar-se à actividade de associação de conteúdos em geral, isto é, independentemente de ser praticada por um prestador de serviços intermediários ou por qualquer outro interveniente na rede. Assim, por actuarem em planos diferentes, inexistente qualquer contrariedade entre estes dois artigos.

Tendemos a discordar desta posição e entendemos estar perante uma verdadeira contradição do legislador nacional. Por um lado, do ponto de vista sistemático, quer o artigo 17.º quer o artigo 19.º encontram-se no mesmo capítulo do RJCE, isto é, o Capítulo III destinado à responsabilidade dos prestadores de serviços em rede. Por outro lado o n.º1 do artigo 19.º refere expressamente a palavra “prestador”, o que necessariamente terá de abranger também os prestadores de serviços intermediários. Assim, se por um lado o artigo 17.º do RJCE obriga o prestador intermediário de associação de conteúdos a impossibilitar o acesso a um conteúdo ilícito mal tenha conhecimento do mesmo, o artigo 19.º do RJCE permite que, ainda que o prestador intermediário tenha conhecimento do conteúdo ilícito no *site* de destino, a sua actividade não seja considerada ilícita.

Como resolver esta contradição? Adoptando o critério hermenêutico da especialidade da norma (*lex specialis derogat legi generali*)²¹⁷ entendemos que a norma do n.º1 do artigo 19.º não pode ser aplicável aos prestadores de serviços intermediários de associação de conteúdos, mas apenas é aplicável aos prestadores de serviços não intermediários, isto é, aos fornecedores de conteúdos que coloquem conteúdos na rede mediante remuneração ou, pelo menos, no âmbito de uma actividade económica, na sequência de pedido individual do

²¹⁵ Cfr. artigo 16.º n.º1 *ex vi* artigo 17.º, todos do RJCE.

²¹⁶ *Vide Lei do Comércio Electrónico Anotada*, p. 63 (anotação ao artigo 17.º, ponto 3).

²¹⁷ A este respeito *vide* JOÃO BAPTISTA MACHADO, *Introdução ao Direito e ao Discurso Legitimador*, pp. 170 ss.

destinatário²¹⁸. Assim, os prestadores de serviços intermediários de associação de conteúdos estarão sujeitos ao regime do artigo 17.º, ou seja, serão obrigados a impossibilitar o acesso a conteúdos ilícitos para os quais os seus *links* ou *motores de busca* remetam, a partir do momento em que tenham conhecimento da ilicitude manifesta dos mesmos. Com efeito, a norma do artigo 17.º, porque só aplicável à intermediação de serviços de associação de conteúdos, derroga, quanto a este aspecto, o disposto no n.º1 do artigo 19.º, uma vez que este artigo diz respeito à actividade de prestação de serviços de associação de conteúdos em geral.

O disposto no n.º2 do artigo 19.º refere as situações em que a própria associação de conteúdos em si – aqui já não nos encontramos a falar da actividade em geral mas da hiperligação em concreto feita – é ou não ilícita. Segundo o normativo, “a remissão é lícita se for realizada com objectividade e distanciamento, representando o exercício do direito à informação, sendo, pelo contrário, ilícita se representar uma maneira de tomar como próprio o conteúdo ilícito para que se remete.” O n.º 3 refere circunstâncias que poderão ajudar o julgador – intérprete a descortinar se, no caso em concreto, o prestador entendeu tomar como seu o conteúdo para o qual remete ou não.

11.7. A solução provisória de litígios

Nos termos do disposto no artigo 18º do RJCE, é consagrada uma solução provisória de litígios, prevista para possibilitar a um potencial lesado um mecanismo extrajudicial que lhe permitisse a retirada provisória do conteúdo ilícito da Internet, naqueles casos de recusa por parte do prestador de serviços intermediários, e de forma célere, de modo a limitar os efeitos do dano, conforme referido no seu n.º2²¹⁹.

Por outro lado, este mecanismo serve o propósito contrário, isto é, também pode ser utilizado para garantir ao proprietário dos conteúdos que sejam retirados que este se oponha a tal acção, advogando pela manutenção dos conteúdos na Internet, como resulta do disposto no n.º3.

²¹⁸ Cfr. n.º1 do artigo 3.º do RJCE. Na verdade, não serão abrangidos pelo disposto no artigo 19.º os fornecedores de conteúdos que o façam a título meramente lúdico, sem fim económico, como sucede com a maior parte dos utilizadores de internet. Isto porque o âmbito de aplicação do RJCE é, como vimos, a regulação da prestação de serviços da Sociedade da Informação.

²¹⁹ Tal mecanismo é apenas aplicável aos casos de armazenagem principal ou associação de conteúdos, conforme resulta do disposto no n.º 1 do artigo 18.º RJCE.

A solução definitiva do litígio, no entanto, apenas pode ser realizada pela via judicial, nos termos do disposto no n.º 7 do artigo 18.º do RJCE²²⁰.

Curiosamente, embora o RJCE preveja, no n.º 4 do citado artigo, que o procedimento do uso desta solução provisória de litígios será especialmente regulamentado, certo é que, até à presente data, nunca entrou em vigor tal regulamentação. Este mecanismo permanece assim, até ao presente momento, uma agradável criação legislativa no texto legal, sem ter sido, ainda, efectivamente implementado na prática.

12. Enquadramento dogmático da responsabilidade civil dos intermediários

12.1. Enquadramento da responsabilidade civil dos intermediários como responsabilidade por acção ou omissão

Não sendo a actividade do intermediário de serviços *online* enquadrada numa das causas de isenção de responsabilidade, será este responsabilizado nos termos gerais, como referido *supra*²²¹.

Resta-nos indagar se a responsabilidade assacada ao intermediário será uma responsabilidade por acção ou por omissão.

No que toca aos serviços de mero transporte de informações ou de acesso à rede, tal não apresenta dificuldades de maior, na medida em que o RJCE prevê uma isenção de cariz objectivo, determinando a actividade em concreto que se encontra isenta de responsabilidade. Assim, se o intermediário se afastar dessa actividade, designadamente por intervir no conteúdo das mensagens que transmite, se esse conteúdo for ilícito o intermediário será responsabilizado por acção pelos danos que causar.

No que toca aos serviços de armazenagem²²², a questão de sabermos se estamos perante uma responsabilidade por acção ou uma responsabilidade por omissão não é simples, desde logo porque o artigo 12.º do RJCE estabelece a ausência de um dever geral de vigilância do conteúdo das informações transmitidas pelos prestadores de serviços intermediários. Da falta deste dever geral de vigilância poderia, então, concluir-se pela não existência da possibilidade

²²⁰ Vide, sobre esta matéria, CLÁUDIA TRABUCO, *op. cit.*, p. 491 ss.

²²¹ Vide p. 81.

²²² E, por via de remissão do artigo 17.º do RJCE para o artigo 16.º do mesmo regime, o que aqui dissermos a respeito dos intermediários de armazenamento principal valerá também para os intermediários de associação de conteúdos.

de responsabilidade civil por omissão dos intermediários²²³, na medida em que o âmbito da ilicitude na omissão é mais exigente do que ao nível da acção, sendo necessário que sobre o omitente incida o dever jurídico de agir²²⁴.

Salvo o devido respeito por opinião contrária, não sufragamos tal entendimento. A responsabilidade pela actividade de armazenamento é uma responsabilidade por omissão, como demonstraremos de seguida.

O artigo 486.º do CC dispõe que “As simples omissões dão lugar à obrigação de reparar os danos, quando, independentemente dos outros requisitos legais, havia, por força da lei ou do negócio jurídico, o dever de praticar o acto omitido.” Ora, como aponta PEDRO NUNES DE CARVALHO, “(...) a referência à lei como fonte do dever jurídico de agir não deve ser interpretado como designando restritivamente a lei civil, deve, pelo contrário, ser entendido no sentido amplo da ordem jurídica.”²²⁵. Para tal contribuem dois fortes argumentos: por um lado, atento o disposto no n.º3 do artigo 9.º do CC, se o legislador optou, no artigo 486.º, por falar em “lei” e não em “lei civil”, então deve o intérprete considerar que a referência é para toda a legislação existente e em vigor no ordenamento jurídico português; por outro lado, esta é a única posição conciliável com o princípio da unidade da ordem jurídica.

Sendo assim, resulta claro que as normas dos artigos 15.º e 16.º do RJCE não são meros “filtros” à responsabilidade civil dos intermediários, mas verdadeiras normas, integrantes do ordenamento jurídico português, que impõe deveres de conduta com relevância prática²²⁶.

Relativamente à armazenagem temporária, o RJCE impõe ao prestador intermediário que actualize a informação segundo as regras usuais do sector, bem como retire ou impossibilite imediatamente o acesso a um conteúdo que saiba ter sido retirado da fonte originária. Quanto à armazenagem principal, os deveres que se impõe ao intermediário são os de, logo que tenha conhecimento da existência de um conteúdo alojado no seu servidor, cuja ilicitude seja manifesta, o retirar ou impossibilitar o seu acesso, logo que possível.

Do *supra* exposto resulta também que, nos casos de armazenagem, onde estejam em causa as violações dos referidos deveres de agir, a prova dessas violações equivalerá também à prova dos requisitos da responsabilidade civil a que os mesmos estão adstritos: facto,

²²³ Neste sentido *vide* PEDRO ROMANO MARTINEZ, *op. cit.*, pp. 271 ss e MIGUEL PEGUERA POCH, *op. cit.*, pp. 35 ss.

²²⁴ *Vide* PEDRO PITTA E CUNHA NUNES DE CARVALHO, *Omissão e dever de agir em Direito Civil*, p. 136.

²²⁵ *Op. cit.*, pp. 144 ss.

²²⁶ Neste sentido *vide* SANTIAGO CAVANILLAS MÚGICA, *op. cit.*, p. 51, n. 3 e GIUSEPPE CASSANO, *op. cit.*, pp. 354 ss.

ilicitude e culpa. Pelo que, demonstrada que esteja a violação dos deveres de agir, apenas bastará ao lesado demonstrar os danos que teve e o nexo causal entre estes e a violação daqueles deveres. Demonstrados que estejam os cinco requisitos da responsabilidade civil, o intermediário de armazenamento incorrerá em responsabilidade civil por omissão.

12.2. Extensão dos deveres de agir que impendem sobre os intermediários?

Como vimos, o RJCE consagra alguns deveres de agir que os intermediários, *maxime*, de armazenamento e de associação de conteúdos, são obrigados a cumprir de modo a não poderem ser responsabilizados civilmente por conteúdos ilícitos difundidos através dos seus sistemas. A questão que se coloca é a seguinte: será possível estender os deveres de agir a outras situações que não as expressamente previstas nos artigos 14.º a 17.º do RJCE?

Desde logo, o artigo 13.º do RJCE, como vimos, impõe deveres genéricos que deverão ser cumpridos por todos os prestadores de serviços intermediários. Assim, a violação de tais deveres também poderá levar à responsabilidade civil dos intermediários²²⁷, quando essa violação se consubstancie num dano para um terceiro.

Questão mais complexa será a de saber se podem ser impostos aos intermediários outros deveres que não os previstos no RJCE.

O considerando n.º 48 da DCE refere que nada impede os Estados-Membros de exigirem dos prestadores de serviços que “exerçam deveres de diligência que podem razoavelmente esperar-se deles.” Entendemos, no entanto, que a imposição de outros deveres de conduta aos intermediários terá de ser feita em termos muito restritos, atento o disposto no artigo 12.º do RJCE – ausência do dever geral de vigilância.

Entendemos que, em certas situações, em que o conteúdo ilícito foi introduzido por um terceiro na rede mas apenas por causa de uma determinada omissão do prestador de serviços intermediários, o intermediário poderá ser responsabilizado com base na omissão de um dever geral de cuidado, que não se encontra taxativamente previsto no RJCE. Pense-se, por exemplo, no caso em que um vírus é introduzido numa rede social apenas por culpa (negligente) do intermediário que não procedeu à actualização do *software* de protecção do

²²⁷ E, neste caso, não só dos intermediários de armazenamento e de associação de conteúdos mas também de mero transporte e de acesso à rede.

seu servidor. São as chamadas situações de ingerência²²⁸, isto é, situações em que a fonte de perigo é criada pelo sujeito sobre o qual acaba por impender a obrigação de auxílio²²⁹.

As situações *supra* referidas, em nosso entender, não consubstanciam uma violação do artigo 12.º do RJCE, pelo que poderão (e deverão) ser exigidas dos prestadores de serviços intermediários.

12.3. A distribuição do ónus da prova

Da leitura das normas de isenção de responsabilidade previstas no RJCE, parece resultar, em nosso entender, que o *onus probandi* da exclusão dos regimes de isenção relativamente a uma actuação em concreto dos intermediários pertencerá sempre ao lesado²³⁰. Não dispondo o RJCE nada em contrário, aplicar-se-á o regime comum do ónus da prova presente no n.º1 do artigo 342.º do C. C..

Com efeito, caberá ao lesado alegar os factos que demonstram as causas que permitem a exclusão da isenção da responsabilidade dos intermediários. Em particular, no que respeita aos serviços de *hosting*, que assumem uma particular relevância na matéria dos CGU, caberá não só ao lesado provar que o intermediário teve conhecimento de que alojava um conteúdo ilícito mas também que nada fez para o retirar ou impossibilitar o acesso a tal conteúdo. Tal ónus probatório afigura-se demasiado exigente se tivermos em conta que o lesado geralmente não possuirá os meios suficientes para demonstrar circunstâncias que normalmente apenas são conhecidas no interior da estrutura empresarial de cada intermediário.

Não obstante, logrando o lesado provar as causas de exclusão dos regimes de isenção, passará a aplicar-se o regime comum da responsabilidade civil, pelo que, em alguns casos, poderá o lesado beneficiar de inversões do ónus da prova, como, por exemplo, caso seja aplicável *in casu*, o regime da responsabilidade obrigacional.

²²⁸ Sobre este aspecto vide PEDRO NUNES DE CARVALHO, *op. cit.*, pp.224 ss.

²²⁹ Relativamente ao exemplo dado, refira-se que, a este respeito, já se pronunciou a Câmara dos Lordes britânica, no sentido de normativizar a obrigação dos prestadores de serviços intermediários velarem pela segurança, no *Primeiro relatório sobre a segurança pessoal na Internet* de 10 de Agosto de 2007. Do mesmo modo se pronunciou também a ENISA (Agência Europeia para a Segurança das Redes e Informação), através do seu relatório intitulado *Segurança, Economia e Mercado Interno* (31.01.2008).

²³⁰ No mesmo sentido LUCÍA MARÍN PEIDRO, *op. cit.*, p. 97. Em sentido divergente, considerando que, no que toca aos serviços de armazenagem principal, o ónus da prova pertence ao intermediário, vide ALBERTO PARENTI, “L’armonizzazione comunitária in matéria di commercio elettronico”, in *Il Commercio elettronico. Profili giuridici e fiscali internazionali*, p. 90. No entanto, como referido em texto, consideramos que no plano vigente não é possível retirar da letra da lei (quer do RJCE quer da DCE) qualquer inversão do ónus da prova.

12.4. Conciliação da responsabilidade civil dos intermediários de armazenamento com a responsabilização do utilizador responsável pela colocação do conteúdo ilícito online

Na hipótese de o autor do acto ilícito (v.g. o utilizador que coloca o conteúdo ilícito *online*) ser identificado e, ao mesmo tempo, existir violação de deveres de conduta por parte do intermediário de armazenamento (v.g. a não remoção do conteúdo, embora conhecendo a sua existência), *quid juris* quanto à responsabilidade?

Nos termos do disposto no n.º1 do artigo 497.º do CC, se forem várias as pessoas responsáveis pelos danos é solidária a sua responsabilidade. A razão do instituto da solidariedade entre os agentes causadores do dano assenta no facto de nem sempre ser possível discernir a exacta participação causal de cada um deles na produção do dano. Não obstante, se, no caso em concreto, for possível diferenciar a participação causal entre cada um dos agentes então o regime aplicável será o da conjunção.

Relativamente à colocação e difusão de conteúdos ilícitos *online*, o utilizador que coloca o conteúdo será responsável pelos danos que o mesmo causar, nos termos expostos *supra*²³¹. Já o intermediário será apenas responsável pelos danos causados pela permanência do conteúdo ilícito no seu servidor depois do seu conhecimento efectivo²³². Assim, à primeira vista pode parecer que o regime da solidariedade se encontra afastado. No entanto, entendemos que não. O utilizador primitivo será sempre responsável por todos os danos que forem causados pelo conteúdo por si colocado na rede. Nada obsta a que o intermediário, mesmo que só seja responsável a partir do momento em que tem conhecimento do conteúdo ilícito e nada faz para o remover, não possa ser responsabilizado solidariamente com o utilizador no pagamento da indemnização total ao lesado. Posteriormente, terá direito de regresso relativamente ao montante indemnizatório pago em excesso quanto à parcela dos danos e da culpa que apenas recairiam sobre o utilizador²³³.

²³¹ Vide Cap. II.

²³² Poderemos considerar também uma eventual responsabilidade do intermediário por posteriores difusões do conteúdo alojado no seu servidor feitas por terceiros, à semelhança do que dissemos para o utilizador primitivo, Vide p. 62.

²³³ Vide, embora em sentido um pouco divergente do nosso, considerando apenas haver condenação solidária relativamente aos danos que tenham sido causados por ambas as condutas, SANTIAGO CAVANILLAS MÚGICA, *op. cit.*, p. 61. Por outro lado, considerando haver responsabilidade solidária, embora apenas relativamente aos chamados *news group*, vide GIUSEPPE CASSANO, *op. cit.*, pp. 116 ss.

13. Análise crítica da solução legal acolhida

13.1. A necessidade da precisão dogmática dos conceitos normativos do artigo 16.º RJCE

Facilmente nos apercebemos que o artigo 16.º do RJCE, em particular os seus n.ºs 1 e 2, possuem conceitos demasiado genéricos. Desde logo se colocam, quanto ao normativo do n.º1, três questões: em que moldes se pode considerar que o intermediário tem conhecimento do conteúdo ilícito? Como determinar a ilicitude manifesta? Finalmente, qual o grau de celeridade exigido ao intermediário quanto à remoção do conteúdo ilícito? Depois, no n.º 2 do referido artigo 16.º, também não se verifica qualquer delimitação dos termos em que o intermediário tem ou deveria ter conhecimento do conteúdo ilícito.

O ordenamento jurídico português, à semelhança do que sucedeu com a DCE, não delimitou normativamente o sentido a atribuir aos conceitos *supra* referidos. Incumbirá, pois, à doutrina e jurisprudência concretizá-los em face do caso em concreto.

a) A problemática do conhecimento do conteúdo ilícito

A expressão “conhecimento” presente no normativo referido parece, à partida, mais abrangente do que a expressão, presente na DCE, de “conhecimento efectivo”. No entanto, em nosso entender, a expressão constante da norma nacional terá de ser interpretada com o sentido dado pela DCE, ou seja, não poderá ser mais ampla que esta, sob pena de nos encontrarmos a violar o disposto no artigo 12.º do RJCE (ausência do dever geral de vigilância).

Não parece haver dúvidas que, nos casos em que o prestador de serviços tem conhecimento por si próprio (ou através de um funcionário seu) do conteúdo ilícito, tal não deixará de ser considerado “conhecimento efectivo” para os efeitos do disposto no n.º1 do artigo 16.º do RJCE. Questão diversa é saber em que moldes consubstancia o “conhecimento efectivo” quando é adquirido por outra via que não o conhecimento próprio.

Relativamente a este último aspecto, o ordenamento jurídico espanhol entende que o intermediário terá “conhecimento efectivo” quando tiver existido uma decisão de um organismo competente que tenha declarado a ilicitude do conteúdo e tenha ordenado a sua

retirada ou a impossibilitação do acesso ao mesmo, bem como a existência de uma sentença judicial que seja do conhecimento do prestador de serviços²³⁴.

O ordenamento jurídico espanhol, ao contrário do nacional, optou por inserir no diploma legal de transposição o seu entendimento sobre o que seria “conhecimento efectivo”, acabando por adoptar uma noção mais restritiva que a adoptada pelo ordenamento jurídico português. Assim, se é certo que a comunicação pelas entidades oficiais se considerará “conhecimento efectivo” para efeitos do nosso diploma legal, tal não significa que se restrinja apenas a estas situações.

Com efeito, a redacção genérica dada ao artigo do RJCE aparenta admitir outras formas de “conhecimento efectivo”, nomeadamente as reclamações efectuadas por terceiros ao intermediário. No entanto, como questiona ALEXANDRE CRUQUENAIRE: Para que exista este conhecimento efectivo do conteúdo ilícito bastará uma qualquer reclamação provida de um terceiro? Tem essa reclamação de justificar minimamente a ilicitude do conteúdo? A reclamação para ser considerada deverá ser assinada (nomeadamente através do uso da assinatura electrónica digital) ou bastará um *e-mail* anónimo²³⁵?

No sistema norte-americano, o DMCA dispõe que a recepção pelo prestador de serviços de uma notificação por parte de um terceiro constitui “conhecimento efectivo” do conteúdo. Não obstante, o DMCA impõe certos requisitos legais para que a notificação seja válida, tentando, de certa forma, impedir que o prestador se veja “inundado” de reclamações sem fundamento. Assim, nos termos do disposto na alínea a) do n.º 3 da secção 512 C) do DMCA, torna-se necessário que a notificação do conteúdo ilícito tenha os seguintes elementos:

- A assinatura, física ou electrónica, do proprietário do direito de *copyright* ou de alguém autorizado a actuar em seu nome;
- A identificação da(s) obra(s) protegida(s) cujos direitos de *copyright* foram violados;
- A identificação do material que se encontra a violar o *copyright* da obra e cuja remoção se solicita, bem como qualquer outra informação que permita ao intermediário localizar razoavelmente o material;
- Informação razoavelmente suficiente que permita ao intermediário contactar a parte reclamante, tal como um endereço de domicílio, número de telefone e, se disponível, endereço de e-mail;

²³⁴ Cfr. artigo 16.º da *Ley 34/2002, de 11 de Julio, de servicios de la sociedad de la información y de comercio electrónico*.

²³⁵ Vide ALEXANDRE CRUQUENAIRE, “Transposition of the e-commerce directive: some critical comments”, in *Direito da Sociedade da Informação*, Vol. V, p. 104.

- Uma declaração de que a parte reclamante se encontra convicta de que o uso do material reclamado não é autorizado pelo dono da obra, pelo seu agente, ou pela lei;
- Uma declaração de que a notificação é verdadeira e que, sobre punição de perjúrio, a parte reclamante, caso não seja o próprio autor da obra violada, está autorizada a actuar em seu nome.

A alínea b), do n.º 3, da secção 512 C) do DMCA, por sua vez, estatui que a notificação que não cumpra os requisitos referidos na alínea anterior não pode ser considerada para efeitos de prova do “conhecimento efectivo” do material ilícito por parte do intermediário de serviços. Porém, caso as falhas da notificação digam apenas respeito à falta de assinatura (física ou electrónica) e/ou à falta da declaração de veracidade da notificação, esta só é excluída para efeitos de prova do “conhecimento efectivo” caso o intermediário tente prontamente contactar a pessoa que elaborou a notificação ou tome outros passos razoáveis para procurar completar a notificação, de modo a que esta obedeça a todos os requisitos referidos *supra*.

O ordenamento jurídico norte-americano consegue dar-nos, assim, algumas pistas sobre a admissibilidade de uma notificação feita por terceiro que possa ser considerada válida para efeitos de prova do “conhecimento efectivo”. Os tribunais norte-americanos também têm vindo a considerar que a existência de documentos internos da empresa intermediária em que se discuta o conteúdo ilícito pode também provar o “conhecimento efectivo”²³⁶.

Face ao exemplo norte-americano, embora apenas aplicável à remoção de conteúdos que violem *copyright*, entendemos que, no que toca ao RJCE, as reclamações provindas de terceiros para os intermediários podem fazer prova do “conhecimento efectivo” do intermediário quanto à existência de um conteúdo ilícito armazenado pelo mesmo. Todavia, a reclamação deverá ter os elementos suficientes e necessários para que o intermediário possa remover o conteúdo com fundada certeza na sua ilicitude²³⁷, desde logo: identificação completa do lesado, os dados para o seu contacto bem como da pessoa que efectua a reclamação (caso não seja o próprio lesado), caso não seja o próprio lesado; identificação do conteúdo ilícito e informações sobre a sua localização (por exemplo, indicação do *link* que faz a ligação ao conteúdo); indicação, ainda que sucinta, do(s) direito(s) violado(s) pelo conteúdo e razões da(s) sua(s) violação(ões). Quanto a outros formalismos, entendemos que bastará o envio de um *e-mail* para o intermediário (embora necessariamente com aviso de recepção, de

²³⁶ Sobre este aspecto *vide* ERIK VALGAEREN e NICOLAS ROLAND, *op. cit.*, p. 216.

²³⁷ Não obstante a isenção de responsabilidade prevista no artigo 18.º, n.º6, do RJCE, relativamente à remoção de conteúdos lícitos, como aludimos *supra*, pp. 86 ss.

modo a constituir prova de que o intermediário recebeu o *e-mail*), sem necessidade de assinatura electrónica ou física. Isto porque, por um lado, entendemos que tal só poderá ser exigido caso exista uma implementação legal dos formalismos a observar no envio da notificação e posterior retirada do conteúdo (*notice and take-down procedures*), por outro lado, incumbe ao intermediário, após a recepção da notificação, contactar o reclamante, de modo a ser esclarecido da autenticidade da reclamação.

Não obstante as indicações dadas, entendemos crucial, por necessário, não só para efeitos de harmonização comunitária e internacional (nomeadamente com o sistema norte-americano), mas também por questões de segurança e certeza jurídicas, a regulamentação legal dos formalismos a que uma notificação de um conteúdo ilícito tenha de obedecer. Tal como refere ALEXANDRE CRUQUENAIRE, a regulamentação legal do sistema de notificação e de retirada dos conteúdos facilita a resolução da questão do “conhecimento efectivo” e não se encontra excluída do âmbito de regulamentação autónoma dos Estados – Membros²³⁸.

Por sua vez, o disposto no n.º 2, do artigo 16.º do RJCE, unicamente aplicável à responsabilidade civil dos intermediários, fala no que, em linguagem anglo-saxónica, vulgarmente é designado de *apparent knowledge* ou *constructive knowledge*.

Mais uma vez torna-se útil averiguar o que se passa noutros ordenamentos, nomeadamente no ordenamento norte-americano, relativamente aos casos em que o intermediário “devia ter conhecimento” do conteúdo ilícito.

No ordenamento norte-americano, a secção 512 C), n.º 1, alínea a), ii) do DMCA, propõe uma base para o “conhecimento aparente”, referindo que “o prestador de serviços não será responsável se (...) na ausência de conhecimento efectivo, não tenha conhecimento de factos ou circunstâncias dos quais possa resultar a aparência de uma actividade ilícita.”. A doutrina e jurisprudência norte-americanas têm apelidado tais factos de *red flags*, ou seja, quando existir uma *red flag*, o intermediário tem a obrigação de a conhecer, não ficando isento de responsabilidade. No entanto, como salientaram os tribunais norte-americanos, o conhecimento genérico de que actividades ilegais podem ocorrer não é suficiente para se

²³⁸ *Op. cit.*, p. 104. O artigo 21.º da DCE, no seu n.º2, refere que os relatórios sobre a aplicação da directiva deverão analisar, entre outras questões, a necessidade de propostas relativas à regulação de procedimentos de *notice and take down*.

considerar que o intermediário devia conhecer o conteúdo ilícito alojado²³⁹. Tal vai de encontro ao disposto no n.º 2, do artigo 16.º do RJCE, na medida em que obriga o juízo do “conhecimento aparente” a ser feito mediante as circunstâncias concretas que o intermediário conhece.

No entanto, já assim não será se, por exemplo, num determinado fórum fornecido por um intermediário, os seus utilizadores discutem abertamente a troca de material protegido por *copyright*, enquadrando-se tal situação num dos casos de *red flag* e, por isso, comprovadores do “conhecimento aparente” por parte do intermediário. De igual forma, o facto de o intermediário voluntariamente “fechar os olhos” a actividades ilícitas que decorram no seu *site* constitui também “conhecimento aparente”²⁴⁰.

Outro exemplo de uma situação em que o intermediário devia ter conhecimento do conteúdo manifestamente ilícito sucede quando um utilizador contrata um serviço de *hosting* (armazenamento) e disponibiliza nesse espaço várias obras protegidas por Direito de Autor (p.e. músicas, filmes, etc...) que acabam por ser descarregadas por outros utilizadores com uma maior frequência do que outros conteúdos (lícitos) disponibilizados no servidor. Neste caso, o servidor do intermediário regista um aumento exponencial do fluxo de transferência de dados face ao habitual, pelo que, entendemos que o intermediário tem o dever de procurar saber a que é que se deve tal aumento. Caso não o faça, incorrerá em responsabilidade civil, pois devia ter conhecimento dos conteúdos ilícitos que estavam disponibilizados no seu servidor²⁴¹.

Da mesma forma, a disponibilização num determinado *site*, cuja propriedade é de um intermediário, de conteúdos cujas descrições façam referência a “ilegal”, “roubado”, ou possuam títulos de filmes ou músicas, entre outros..., podem configurar também a responsabilização do intermediário por dever ter conhecimento daqueles conteúdos. Não obstante, tudo dependerá do caso em concreto, pois, como já foi alertado na jurisprudência

²³⁹ *Corbis, Inc. v. Amazon.com* (2004), onde a *Amazon* tinha sido demandada por existirem no seu *site* vendedores que se encontravam a vender *online* posters de trabalhos protegidos pelo *copyright*, propriedade da *Corbis*. O tribunal absolveu a *Amazon*, entendendo que, de acordo com a matéria provada, não tinha resultado a prova de que a *Amazon* tinha ou deveria ter conhecimento do material ilícito. Vide ERIK VALGAEREN e NICOLAS ROLAND, *op. cit.*, pp. 216 ss.

²⁴⁰ ERIK VALGAEREN e NICOLAS ROLAND, *op. cit.*, p. 217.

²⁴¹ A este respeito veja-se JOEL TIMÓTEO RAMOS PEREIRA, *Compêndio...*, pp. 881 ss. e ainda JANE C. GINSBURG, “Whose tube? Liability risks and limitations of copyright-dependent technology entrepreneurs”, in *Google et les nouveaux services en ligne: impact sur l'Économie du contenu et questions de propriété intellectuelle*, p. 236. De igual forma, LILIAN EDWARDS, *op. cit.*, p. 67, sugere que um intermediário que se dedique a alojar grandes quantidades de CGU, onde a ilegalidade de muitos deles é genericamente conhecida, tem necessariamente de conhecer o conteúdo ilícito, constituindo este também um dos casos de “conhecimento aparente”.

norte-americana, nomeadamente no caso *Perfect 10, Inc. v. CCBill LLC*²⁴², o uso de tais expressões pode significar apenas uma tentativa de tornar os conteúdos mais apelativos para serem descarregados, sem querer verdadeiramente significar que os mesmos são ilegais²⁴³.

Assim, torna-se evidente que a determinação das situações em que o intermediário devia ter conhecimento da ilicitude manifesta de um determinado conteúdo não é susceptível de ser taxativamente tipificada, mas, ao invés, deverá ser apurada de acordo com as circunstâncias concretas de cada caso, nomeadamente com o auxílio do critério do *bonus pater familiae*, delineando se, no caso em concreto, um normal prestador de serviços, face aos conhecimentos que detinha, teria ou não tomado conhecimento do conteúdo e se o removeria, caso tal conteúdo fosse manifestamente ilícito. Não obstante, apresentámos aqui algumas situações onde se constata a existência do “conhecimento aparente”.

b) A ilicitude manifesta

O artigo 16.º do RJCE é enquadrado tendo por base a ilicitude manifesta de um determinado conteúdo, na medida em que só existindo essa ilicitude manifesta é que o intermediário de serviços será responsável. O regime jurídico não determina, contudo, o que se pode entender por ilicitude manifesta. O adjetivo “manifesto” significa aquilo que é claro, evidente, notório, cuja existência ou natureza é incontestável. Assim, na avaliação da situação por parte da entidade responsável – *in casu* o intermediário de serviços – se subsistirem dúvidas sobre a sua ilicitude então o conteúdo não será manifestamente ilícito e, por isso, não caberá ao intermediário qualquer dever de o retirar.

Não obstante a solução acolhida, entendemos que, em termos práticos, tal levará a uma grande insegurança por parte dos intermediários quanto à remoção ou não do conteúdo em causa. Se não existem dúvidas de que os conteúdos relacionados com pornografia infantil, actos de terrorismo, ódio racial e xenofobia constituem casos de ilicitude manifesta, em casos relacionados com a violação de direitos de autor, ofensas ao bom nome, à imagem, à reserva da intimidade da vida privada, entre outros, a ilicitude dos mesmos já poderá ser mais difícil de detectar. Nestas hipóteses, o intermediário não tem uma base legal na qual possa apoiar a sua decisão de retirada ou não retirada do conteúdo, sendo que, caso o intermediário não retire o conteúdo por ter dúvidas sobre a sua ilicitude, e este seja declarado manifestamente ilícito, nomeadamente pelo ICP-ANACOM, de acordo com o artigo 18.º do RJCE, o intermediário

²⁴² *Perfect 10, Inc. v. CCBill LLC* (2007).

²⁴³ Vide JANE C. GINSBURG, *op. cit.*, pp. 236 ss.

poderá ser sujeito a responsabilidade civil. De igual forma, caso o intermediário opte pela sua retirada e o conteúdo seja declarado manifestamente lícito, também aqui poderá ser responsabilizado perante o interessado que colocou o conteúdo *online*²⁴⁴.

Assim, em nosso entender, seria útil, principalmente com finalidades de segurança e certeza jurídicas, uma regulamentação posterior dos casos, ainda que exemplificativa, em que exista ilicitude manifesta.

c) Determinação da diligência exigida quanto à retirada do conteúdo ilícito após a notificação da sua existência

Outra dúvida que o RJCE deixa por esclarecer diz respeito ao período de tempo espectável para que o intermediário retire o conteúdo manifestamente ilícito, após a recepção da notificação da sua existência. O RJCE não impõe qualquer tipo de prazo para a retirada do conteúdo após a recepção da notificação²⁴⁵. Qual o prazo razoável para poder aferir que o intermediário agiu com a diligência exigível?

Mais uma vez o juízo deverá ser efectuado tendo em conta as circunstâncias no caso em concreto, à luz do critério do *bonus pater familiae*. Serão, nomeadamente, circunstancialismos relevantes para a apreciação do cumprimento do prazo de actuação: o número de servidores que o intermediário tem à disposição dos utilizadores; o número de utilizadores; o número de conteúdos que se encontram alojados no(s) servidor(es) do intermediário; a evolução tecnológica de identificação e localização de conteúdos; a existência ou inexistência de hiperligações que liguem outros *sites* ao conteúdo; entre outros. Assim, o tempo de reacção do intermediário deverá ser maior quanto maior for o grau de complexidade técnica dos serviços que proporciona bem como o número de conteúdos que armazena e, por outro lado, deverá ser reduzido quanto melhor e mais desenvolvidos se encontrarem os mecanismos de pesquisa e identificação dos conteúdos nos seus servidores.

²⁴⁴ Embora, em nosso entender, o intermediário possa depois exigir o que houver pago daquele que tenha procedido à notificação do conteúdo ilícito.

²⁴⁵ Omissão também da Directiva e da Lei espanhola de transposição, como disso nos dá conta JOSÉ MANUEL VILLAR URÍBARRI, “El régimen jurídico de los prestadores de servicios de la sociedad de la información”, in *Derecho de Internet – La Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico*, p. 404.

13.2. Ausência de deveres de diligência para os serviços de mero transporte ou de acesso à rede

O artigo 14.º do RJCE, tal como sucede com o artigo 12.º da DCE, não consagra qualquer obrigação de não proceder à transmissão de uma determinada mensagem ou conteúdo quando se obtiver, por qualquer forma, conhecimento de que o seu conteúdo é ilícito, nos termos do disposto no n.º1 do artigo 16.º do RJCE, ou que foi retirado o acesso ao conteúdo da fonte originária, como dispõe o n.º3 do artigo 15.º do RJCE.

Entendemos que não é possível fazer uma aplicação analógica de qualquer um dos dois preceitos *supra* referidos para abranger também os casos das actividades de *mero transporte* ou de *acesso à rede*. Desde logo por, no nosso entender, não existe qualquer lacuna legal, *in casu*, “lacuna teleológica”, que necessite de ser preenchida. Por isso, não existe a possibilidade de recurso à analogia²⁴⁶. As normas dos artigos 14.º ss. do RJCE são normas apenas aplicáveis aos casos ali especificados e nos moldes em que ali são definidos. Disso nos assegura o legislador comunitário. Vejamos: o considerando n.º 47 da DCE impõe aos Estados-Membros que não consagrem obrigações gerais de vigilância, mas refere que este impedimento não diz respeito a obrigações de vigilância em casos específicos. No entanto, logo no considerando n.º 48, refere-se que podem ser impostos deveres de vigilância aos prestadores de serviços intermediários que “acolham informações prestadas por destinatários dos seus serviços” – isto é o mesmo que dizer “os fornecedores de alojamento”. Ou seja, não consistindo a actividade de mero transporte ou acesso à rede uma actividade de armazenamento para efeitos da DCE e, consequentemente, do RJCE, o legislador quis expressamente afastar a imposição de qualquer dever de diligência aos prestadores de serviços intermediários de transporte e / ou de acesso.

No entanto, não deixa de merecer um lamento, da nossa parte, a falta de consagração legal de um qualquer dever de diligência, como sucede com as restantes actividades de intermediação de conteúdos abrangidas pelo âmbito do RJCE²⁴⁷. Enquanto actividade de natureza eminentemente automática e temporária, em nosso entender carecia de se regulamentar também para estes serviços uma obrigação de, por um lado, utilizar as tecnologias de transporte e acesso segundo as regras habituais do sector, bem como deixar de

²⁴⁶ Sobre a definição de lacunas, em especial, para o que aqui nos importa, das “lacunas da lei” ou “lacunas teleológicas” e a possibilidade de recurso à analogia *vide*, por todos, JOÃO BAPTISTA MACHADO, *op. cit.*, pp. 195 ss.

²⁴⁷ Apontamento este que também é dado por PEDRO PAIS DE VASCONCELOS, “Responsabilidade dos prestadores de serviços em rede”, in *Lei do Comércio Electrónico Anotada*, pp. 285 e 286.

proceder à transmissão do conteúdo quando existisse o conhecimento, por alguma via, de que o mesmo tinha sido retirado de outros locais, independentemente do seu carácter manifestamente ilícito ou não, à semelhança do que sucede para os serviços de *caching*, nos termos do disposto na alínea b) do n.º 2 e no n.º 3, ambos do artigo 15.º do RJCE. Será expectável que o legislador comunitário, em sede de revisão da DCE que tenuemente se anuncia, proceda à alteração do seu artigo 12.º (correspondente ao 14.º RJCE), no sentido de incluir, pelo menos, este dever de diligência.

Actualmente, contudo, parece-nos que apenas se poderá exigir que o intermediário de *mero transporte* ou de *acesso* cesse a transmissão ou acesso a um determinado conteúdo se for para isso notificado através das entidades administrativas ou judiciais próprias, nos termos das obrigações gerais que impendem sobre os intermediários, em especial nos termos do disposto na alínea c) do artigo 13.º do RJCE.

13.3. Ausência da normatização da “ausência do benefício económico directamente derivado da actividade ilícita”

O DMCA, como referimos, para além dos requisitos também existentes na DCE e no RJCE, para o enquadramento da actividade do intermediário numa das causas de isenção de responsabilidade, consagra também o requisito da falta de benefício económico para o intermediário em razão directa da actividade ilícita levada a cabo através do serviço disponibilizado. Esta avaliação do benefício económico resultante da actividade ilícita deve ser determinado com bom senso, de acordo com as circunstâncias do caso em concreto, como bem salienta a Comissão de Justiça do Senado norte-americano²⁴⁸. É discutido, na doutrina e jurisprudência norte-americanas, até que ponto um determinado benefício económico é ou não directamente imputável ao conteúdo ilícito, de modo a excluir os intermediários do regime de isenção²⁴⁹. A esta questão voltaremos *infra*, no ponto 16²⁵⁰.

De todo o modo, esta exclusão não se encontra directamente prevista na DCE, nem no RJCE. Não obstante entendemos, como melhor iremos expor *infra*, que, de acordo com a definição de intermediário de serviços dada pelo diploma português no seu artigo 4.º, n.º5, poderemos considerar que a existência de benefício económico para o intermediário, proveniente directamente da actividade ilegal, afecta a sua neutralidade e independência face

²⁴⁸ *Senate Judiciary Committee Report*, n.º 105.

²⁴⁹ Sobre este aspecto *vide*, entre outros, JANE C. GINSBURG, *op. cit.*, pp. 238 ss.

²⁵⁰ *Vide* pp. 115 ss.

aos respectivos conteúdos – requisitos essenciais da definição de prestador de serviços intermediários – e, por isso, é susceptível de conduzir ao afastamento da aplicabilidade *tout court* das normas de isenção de responsabilidade.

13.4 Potencial conflito entre a retirada dos conteúdos por parte dos intermediários e a liberdade de expressão e informação proporcionada pela Internet

Um último aspecto crítico em relação ao regime vigente diz respeito ao potencial conflito que se poderá suscitar relativamente à obrigação de retirada dos conteúdos manifestamente ilícitos por parte dos intermediários de armazenamento e os direitos à liberdade de expressão e de informação, dois direitos fundamentais consagrados constitucionalmente²⁵¹, que a Internet e, em particular, a *www*, exponenciaram globalmente.

Tal apreensão, apontada sobretudo pelas associações de defesa da liberdade de expressão, entre outras, deriva do facto de o regime vigente colocar os intermediários de armazenamento principal como uma espécie de “polícias da rede” ou, como diria GIUSEPPE CASSANO, uma espécie de “censores telemáticos”²⁵².

Veja-se que, relativamente ao regime português, o intermediário, ao receber uma notificação de um terceiro, encontra-se obrigado a actuar: ou removendo o conteúdo a que a notificação faz referência ou não o removendo, dependendo do intermediário a decisão sobre se o conteúdo é, ou não, manifestamente ilícito. No entanto, se o intermediário não retirar o conteúdo e, posteriormente, ele vier a ser declarado manifestamente ilícito, o intermediário poderá ser responsabilizado. Se, por outro lado, optar por o retirar, ele apenas será responsabilizado face ao utilizador que o colocou se o conteúdo se vier a demonstrar manifestamente lícito, conforme vimos, nos termos do disposto no n.º 6, do artigo 18.º do RJCE²⁵³. Assim, perante a posição do intermediário, em caso de dúvida ele optará sempre por retirar o conteúdo em vez de mantê-lo, uma vez que as hipóteses de ser responsabilizado pela sua remoção serão bastante diminutas.

²⁵¹ Cfr. artigo 37.º da Constituição da República Portuguesa.

²⁵² *Op. cit.*, pp. 377 ss.

²⁵³ O que ocorrerá, em nosso entender, raras vezes, uma vez que a litude manifesta de um conteúdo terá de ser clara, evidente, notória. Ora, quando um terceiro notifica um prestador para a remoção de um determinado conteúdo, já o próprio terceiro configura tal conteúdo como sendo ilícito, pelo que, logo por aqui, a litude manifesta do conteúdo sairá abalada, restando ao prestador averiguar se a ilicitude é ou não manifesta. Só assim não sucederá em casos de notificações manifestamente infundadas que serão, em nosso entender, reduzidas.

Torna-se perigoso deixar nas mãos do intermediário a decisão de manter ou retirar o conteúdo, uma vez que se trata de uma entidade privada cuja finalidade não é ser polícia ou juiz... Não obstante a existência de juristas na estrutura interna de cada intermediário, necessários a uma correcta análise jurídica de cada uma das reclamações que o prestador intermediário receba, estes, em virtude da vinculação que detêm com a empresa prestadora de serviços, certamente pautarão a sua actividade no sentido de assegurar a melhor perspectiva para a empresa e, assim, caso tenham dúvidas (e muitas vezes as terão) optarão por aconselhar a sua imediata remoção.

Neste campo, julgamos encontrar-nos perante uma colisão entre o direito à liberdade de expressão e de informação face ao bem público que será, *prima facie*, a segurança na Internet. Em nosso entender, será admissível uma restrição ao direito da liberdade de expressão e de informação, desde que, como não poderia deixar de ser, proporcional e “restritiva”²⁵⁴.

Entendemos também que tal restrição já se encontra consagrada nos termos do RJCE, uma vez que o legislador, e bem, optou por incluir um mecanismo de solução provisória de litígios que permite almejar a proporcionalidade da restrição verificada, nos termos do artigo 18.º da Constituição da República Portuguesa. Assim, quando um conteúdo for retirado, caso o seu autor entenda que não existiram razões para o efeito, poderá recorrer à ICP / ANACOM que, em 48 horas, terá de dar uma solução provisória ao litígio, o que permite que o utilizador não necessite de esperar por uma decisão judicial para ver de novo o seu conteúdo *online*²⁵⁵.

Esperemos que o legislador nacional depressa colmate a falta de regulamentação do sistema provisório de resolução de litígios para que este possa efectivamente ser posto em prática, uma vez que, como vimos, a sua importância é primordial no sentido de não atribuir à restrição a que se assiste no RJCE um carácter maior do que o inicialmente previsto²⁵⁶.

De todo o modo, os intermediários, ao retirar um conteúdo, deverão sempre ter em conta o eventual direito à liberdade de expressão do respectivo autor que poderá ser afectado com

²⁵⁴ JOSÉ JULIO FERNÁNDEZ RODRIGUEZ, “Seguridad y libertad: ¿equilibrio imposible? Un análisis ante la realidad de Internet” in *Internet: un nuevo horizonte para la seguridad y la defensa – II congreso sobre Seguridad, Defensa e Internet, Santiago de Compostela, noviembre de 2006*, pp. 20 ss., refere mesmo que, por razões de segurança, é possível justificar a restrição de certos conteúdos, no entanto essa restrição deve ser “restrita”, sob pena de introduzir censuras que repugnam a democracia.

²⁵⁵ Nas situações que, como se depreende, não declarem a ilicitude do conteúdo. Caso esta seja declarada, não existe outra forma para o utilizador que a colocou que não seja a de recorrer aos tribunais, *maxime*, a uma providência cautelar ou, até, ao Tribunal Constitucional.

²⁵⁶ Deixaremos de fora deste estudo, por extravasar o âmbito do mesmo, a questão de saber se a falta de regulamentação do referido artigo 18.º do RJCE poderá consubstanciar uma inconstitucionalidade por omissão, na medida em que a implementação efectiva deste artigo é fundamental para que a restrição à liberdade de expressão e informação seja proporcional.

essa remoção, devendo ser sempre ponderado, dentro do possível, um balanço entre a permanência do conteúdo *online* e a eventual ilicitude do mesmo.

14. Breves considerações sobre os contratos de prestação intermediária de serviços na Internet, em particular na web 2.0, e a sua aplicabilidade relativamente a conteúdos ilícitos colocados e difundidos em rede

14.1. A subscrição de serviços da web 2.0. Em particular as cláusulas de exclusão da responsabilidade

Na *web 2.0*., conforme já referido, a grande maioria dos serviços fornecidos pelos prestadores intermediários são gratuitos, sem qualquer custo de adesão para o utilizador-consumidor. Não obstante, tais contratos não deixam de ser celebrados no âmbito de uma actividade económica, pelo que se incluem ainda na definição de “serviço da sociedade da informação”, para efeitos do disposto no n.º1 do artigo 3.º do RJCE²⁵⁷. Assim, tais contratos terão também de obedecer aos formalismos exigidos pelo RJCE, nos termos do disposto nos artigos 24.º ss. que regulam a contratação electrónica²⁵⁸.

Os contratos na *web 2.0* serão, na maioria das vezes, contratos de serviços de armazenamento principal de informação, com maiores ou menores especificidades, uma vez que permitem ao utilizador colocar os seus próprios conteúdos na Internet²⁵⁹.

Nos termos contratuais que geralmente se estabelecem, no que toca à responsabilidade civil pelos conteúdos colocados e difundidos *online*, costumam instituir-se duas cláusulas de relevante importância: a primeira no sentido de que o utilizador-consumidor é responsável por todos os conteúdos e acções que desempenhe com a utilização dos serviços proporcionados pelo prestador intermediário de serviços; a segunda no sentido de que o prestador intermediário de serviços não é responsável pelos danos que possam advir da utilização dos

²⁵⁷ Vide *supra*, p. 80.

²⁵⁸ Não iremos, contudo, analisar com profundidade o regime da contratação electrónica previsto no RJCE, por extravasar o âmbito do presente estudo.

²⁵⁹ O contrato de armazenamento principal será uma espécie de contrato misto de prestação de serviços e locação, não obstante as suas especificidades resultantes da própria natureza digital dos contratos celebrados na Internet. Sobre o contrato de armazenagem em especial vide JOEL TIMÓTEO RAMOS PEREIRA, *Compêndio jurídico...*, pp. 119 ss.

seus serviços, quer por falhas de segurança e de privacidade que possam ocorrer, quer pelos conteúdos colocados pelos seus utilizadores²⁶⁰.

Poder-se-ia assim, *prima facie*, entender que, no campo da responsabilidade obrigacional, os intermediários de serviços sempre excluiriam da sua responsabilidade qualquer acto ilícito desempenhado por um utilizador subscritor do serviço do intermediário. No entanto, a admissibilidade de tais cláusulas à luz do nosso ordenamento jurídico afigura-se-nos duvidosa, na medida em que, via de regra, são nulas as cláusulas que excluam a responsabilidade civil de uma das partes, nos termos do disposto nos artigos 809.º e 800.º, n.º2, do CC e ainda atento o disposto nas alíneas a), b), c) e d) do artigo 18.º do Regime das Cláusulas Contratuais Gerais – Decreto-Lei n.º 446/85, de 25 de Outubro²⁶¹. *In casu*, estas cláusulas serão nulas na medida em que prevejam causas exoneratórias de responsabilidade que vão para além das previstas no RJCE²⁶².

Assim, face ao ordenamento jurídico português vigente, não será pelo facto de se encontrar estipulado no contrato de prestação de serviços intermediários *online* uma cláusula exoneratória de responsabilidade civil que os prestadores não poderão ser responsabilizados. De todo o modo, a questão fulcral a resolver, e que nos irá agora ocupar o estudo, é de saber se, face à colocação e difusão de conteúdos *online*, o prestador intermediário poderá ser chamado a indemnizar o lesado ao abrigo da responsabilidade civil obrigacional.

Desde logo urge diferenciar a responsabilidade obrigacional que poderá hipoteticamente imputar-se aos intermediários. Esta será diferente, consoante o lesado seja o próprio utilizador do serviço, caso em que será parte no contrato, ou, ao invés, seja um terceiro que, não sendo parte no contrato, não utilizando o serviço, sofre danos pelos conteúdos colocados pelos utilizadores do mesmo.

A responsabilidade obrigacional, se aplicável, poderá instituir um mecanismo mais vantajoso para a demanda de eventuais lesados, nomeadamente através da inversão do ónus

²⁶⁰ A título de exemplo, relativamente às cláusulas que costumam constar dos contratos-tipo de acesso e armazenamento de informações na rede, vide VALENTIN CARRASCOSA LÓPEZ, CARLOS FERREYROS SOTO e AUDÍLIO GONZÁLES AGUILAR, *Los contratos en la sociedad de la información – formularios de contratos informáticos e Internet*, pp. 864 ss.

²⁶¹ Neste sentido vide, por todos, ANTÓNIO PINTO MONTEIRO, *Cláusulas limitativas e de exclusão da Responsabilidade Civil*, em especial pp. 391 ss. e ainda, do mesmo autor, “A responsabilidade civil na negociação informática”, in *Direito da Sociedade da Informação*, Vol. I, p. 238.

²⁶² Vide MARÍA NÉLIDA TUR FAÚNDEZ, “La responsabilidad contractual de los intermediarios electrónicos”, in *Deberes y responsabilidades de los servidores de acceso y alojamiento: un análisis multidisciplinar*, pp. 157 ss.

da prova da culpa do devedor no incumprimento²⁶³. E, sendo o lesado considerado parte no contrato, ou susceptível de se considerar protegido por este, o prestador de serviços será responsável caso este incumpra deveres de protecção que, nos termos contratuais, lhe eram exigíveis.

Assumirá, portanto, particular relevância delinear quais serão os deveres de protecção exigíveis aos prestadores de serviços intermediários relativamente aos seus utilizadores e relativamente a terceiros, com base nos contratos de prestação de serviços celebrados²⁶⁴.

14.2. A emergência de deveres de protecção dos prestadores de serviços intermediários face aos consumidores com os quais celebram contratos

Questão inerente à existência de deveres de protecção é saber se, pelo facto de os contratos celebrados serem, na maior parte das vezes, contratos gratuitos, sem necessidade de qualquer prestação pecuniária por parte do utilizador–consumidor dos serviços para a sua utilização, aqueles existem na mesma. Poderá colocar-se a questão de, não sendo exigido ao consumidor qualquer prestação para a celebração do contrato, este também não ter direito a exigir uma especial protecção por parte do prestador de serviços.

No entanto, como já referimos *supra*, a prestação de serviços na Internet, em particular no advento da *web 2.0*, embora seja, à partida, sem custos para o utilizador, poderá ter um escopo lucrativo. Não estamos, por isso, no campo das “relações de simples altruísmo ou de mera obsequiosidade” para eventualmente concluirmos pela ausência de deveres de protecção que devam incidir sobre os intermediários na execução do contrato. A este respeito, CARNEIRO DA FRADA salienta que “(...) boa parte das prestações e transacções gratuitas nos nossos dias se inserem em estratégias económicas mais amplas (...) pelo que também elas realizam de algum modo as características do contacto negocial (...)”²⁶⁵. São essas características, de acordo com o autor, a pugna de interesses e a ausência de atitudes exclusivamente altruístas; a relevância de estratégias económicas; a não predisposição para “complacências” em face das condutas da outra parte²⁶⁶.

²⁶³ Não obsta, no entanto, a que o lesado tenha na mesma de provar as causas de exclusão do regime de isenção de responsabilidade previstas no RJCE.

²⁶⁴ Para uma teoria geral dos deveres de protecção *vide*, por todos, CARNEIRO DA FRADA, *Contrato e deveres de protecção*.

²⁶⁵ *Vide* MANUEL A. CARNEIRO DA FRADA, *Contrato...*, p. 297, n. 605.

²⁶⁶ *Idem, ibidem*.

Ao analisarmos o contrato de prestação de serviços *online* característico da *web 2.0* verificamos que se mantêm as características de um contacto negocial, não obstante a sua estrutura, *rectius* forma, gratuita. Com efeito, o prestador disponibiliza tais serviços de forma aparentemente gratuita de modo a aliciar um maior número de clientes e, conseqüentemente, obter maiores ganhos financeiros, uma vez que o sistema de rendimentos auferidos por força da publicidade alojada nos seus servidores é directamente proporcional ao número de utilizadores que consumam o serviço – assim não poderemos dizer que estamos perante uma atitude altruísta do prestador, mas sim, pelo contrário, perante uma atitude egoísta, de pugna por interesses económicos próprios do intermediário. Em consequência, verificamos que subjaz a este tipo de contratação uma estratégia económica sólida e eficaz, atendendo à evolução rápida que os serviços da *web 2.0* tiveram e estão a ter na Sociedade da Informação. Por fim, não nos parece que os prestadores de serviços intermediários em rede tenham “complacências” para com condutas ilícitas por parte dos seus utilizadores, uma vez que, assim que notificados dos conteúdos ilícitos colocados nos seus servidores, os prestadores intermediários procurarão localizar o conteúdo e retirá-lo, logo que possível²⁶⁷.

Assim, é claro que o incumprimento do estipulado no contrato de prestação de serviços por parte do prestador intermediário resultará na possibilidade de este ser responsabilizado perante o utilizador – parte no contrato – nos termos mais gravosos da responsabilidade obrigacional²⁶⁸.

A questão que se coloca, no que ao nosso estudo diz respeito, prende-se, contudo, em saber se poderá surgir dentro do contrato de prestação de serviços celebrado entre o intermediário e o utilizador um dever do primeiro face ao segundo de o proteger quanto a conteúdos ilícitos colocados por terceiros. Isto porque o próprio utilizador de um serviço pode ser lesado pelo conteúdo colocado por outro utilizador desse mesmo serviço, lesão essa que pode ocorrer quer quanto à propriedade do utilizador (p.e. a disseminação de um vírus que danifica os computadores dos restantes utilizadores do serviço), quer quanto à pessoa do utilizador (p.e. a colocação numa rede social de um comentário que atenta contra o bom nome de um utilizador dessa mesma rede). Como refere CARNEIRO DA FRADA, “Dentro da fenomenologia dos deveres de protecção da integridade [do contrato] avultam, como seu núcleo mais significativo do ponto de vista do relevo histórico-doutrinário, aqueles que

²⁶⁷ O que não significa que não exista “complacência” com as referidas utilizações indevidas, quando exista um conhecimento genérico de que actividades ilícitas podem estar a decorrer nos servidores do intermediário. A falta de “complacência” é, para o que nos interessa, averiguada no caso em concreto, após a notificação do prestador para a existência de determinado conteúdo ilícito no servidor.

²⁶⁸ Vide CARNEIRO DA FRADA, *Contrato...*, p. 277, n.605.

protegem os bens das partes, especialmente propriedade e pessoa, contra lesões perpetradas por outrem”²⁶⁹.

Em nosso entender, existe um dever de protecção dos intermediários face aos utilizadores partes no contrato, no sentido de proteger o respectivo *hardware* de conteúdos que o danifiquem (v.g. vírus) e que sejam colocados e difundidos através dos serviços disponibilizados. Isto porque os serviços disponibilizados pelos intermediários, normalmente plataformas de armazenamento de dados e de interacção entre os utilizadores, são geridos por aqueles, o que determina que só os intermediários tenham o controlo de determinados riscos que possam surgir no âmbito do serviço que prestam, como é o caso da infiltração dos mesmos por vírus. Assim, só o intermediário pode controlar tais riscos ou evitá-los, adoptando a diligência exigida para tal²⁷⁰, mas desde que com critérios de razoabilidade, por exemplo através da utilização de *software* actualizado de defesa contra intrusões alheias e que sejam prática corrente no sector de actividade onde o prestador se encontre inserido. Isto porque uma exigência de maior segurança que a prática instituída no sector (por exemplo, através da implementação dos melhores e mais eficazes sistemas de prevenção actualmente existentes) conflituará com o interesse das partes, *maxime* do intermediário, pois este não configurará, na celebração do contrato de prestação de serviços, a obediência a deveres de protecção que vão para além do imposto na boa-fé que deve pautar a relação entre as partes durante a execução negocial. Apenas o cumprimento dos deveres de cuidado que sejam costumeiros no sector poderá ser exigido ao intermediário, já que são esses mesmos deveres que o utilizador razoavelmente pode esperar do prestador.

De resto, a emergência deste particular dever de protecção não será muito diferente da situação de ingerência apontada no âmbito da responsabilidade extraobrigacional a que aludimos *supra*²⁷¹, com a vantagem inerente ao facto de, sendo o lesado parte no contrato de prestação dos serviços intermediários, poder invocar a violação deste particular dever de protecção e, assim, beneficiar da presunção de culpa do devedor, *in casu* o intermediário, no incumprimento do mesmo.

Quid juris quanto a riscos não contidos no âmbito da esfera de actuação do intermediário? Encontramo-nos a falar não só de conteúdos ofensivos para a pessoa de um determinado utilizador, colocados por outro, mas também de conteúdos que danificam

²⁶⁹ Vide *Contrato...*, pp. 261 ss.

²⁷⁰ Vide CARNEIRO DA FRADA, *Contrato...*, p. 195.

²⁷¹ Vide pp. 92 ss.

hardware e que são disseminados através de mensagens privadas, dissimuladamente²⁷², entre os utilizadores e não colocados no servidor do intermediário. Nestes casos, somos de opinião que não serão exigíveis deveres de protecção do intermediário face ao utilizador parte no contrato, na medida em que aquele já não tem domínio sobre tais riscos decorrentes da própria actividade. O intermediário não pode razoavelmente prever que um ou outro utilizador coloque um conteúdo ilícito na rede que provoque danos na pessoa de outro utilizador, bem como não pode responsabilizar-se por vírus que são concebidos e difundidos de forma a ultrapassar os filtros tecnológicos existentes e actualizados que o intermediário tem no seu *site*. Nestes casos, não se justificará a existência de deveres de protecção. Só assim não será se, porventura, no próprio contrato, o intermediário assumir expressamente a protecção do utilizador face a tais danos. De outro modo, a imposição destes deveres, sem a sua previsão no contrato, sempre consubstanciaria uma violação da obrigação de não vigilância prevista no artigo 12.º do RJCE.

14.3. A emergência de deveres de protecção dos prestadores de serviços intermediários face a terceiros

Questão diversa será averiguar a possibilidade de, com fundamento nos contratos de prestação de serviços intermediários celebrados entre os prestadores e utilizadores, um terceiro solicitar uma pretensão indemnizatória contra o intermediário, devido a danos ocorridos por conteúdos ilícitos colocados e difundidos pelos seus sistemas.

Desde logo, recordemos que, via de regra, os contratos têm eficácia *inter-partes*, pelo que as obrigações assumidas por qualquer uma das partes apenas vinculam a outra e não produzem efeitos face a terceiros²⁷³. Assim, *prima facie*, lesados terceiros não poderão demandar um intermediário com base na violação de deveres de protecção decorrentes do contrato celebrado entre estes e um determinado utilizador. Contudo, poderá colocar-se aqui a questão da aplicabilidade da figura do contrato com eficácia de protecção para terceiros, que tem vindo a ser admitida pela doutrina portuguesa²⁷⁴.

²⁷² Dissimulação que é atingida através do envio de *e-mails* onde o endereço do remetente se encontra falsificado (geralmente coincide com o nome de um dos contactos de *e-mail* da conta para o qual o *e-mail* fraudulento se destina) e, por isso, consegue passar os filtros *anti-spamming* utilizados pelo intermediário.

²⁷³ Sobre a eficácia *inter-partes* do contrato e a não eficácia externa das obrigações *vide* RIBEIRO DE FARIA, *Direito das obrigações*, pp. 33 ss. e 41 ss.

²⁷⁴ A este propósito *vide* JORGE SINDE MONTEIRO, *Responsabilidade por Conselhos, Recomendações ou Informações*, p.518ss. e, ainda, MANUEL A. CARNEIRO DA FRADA, *Uma “Terceira Via” no Direito da*

Esta figura, muitas vezes considerada um tipo mitigado do contrato a favor de terceiros²⁷⁵, impõe a uma das partes, *in casu* os intermediários, a assunção de certos deveres de protecção face a terceiros, por força da natureza do contrato celebrado²⁷⁶. Resulta, no entanto, como elemento essencial para a aplicabilidade desta figura, que seja possível a identificação e circunscrição dos terceiros protegidos²⁷⁷, bem como a existência de uma vontade do devedor em querer proteger tais terceiros.

Apenas quando tais requisitos estejam reunidos é que será possível responsabilizar o prestador face a esses mesmos terceiros, responsabilidade essa que se situará numa zona “cinzenta”, na chamada “terceira via” da responsabilidade civil²⁷⁸.

In casu, regra geral, inexistirá qualquer identificação e circunscrição dos terceiros, atendendo à própria natureza dos serviços prestados na *web 2.0* e à própria escassez de informação prestada pelo utilizador no momento da subscrição desses mesmos serviços, o que impossibilita a circunscrição e identificação pelo prestador intermediário de eventuais terceiros próximos do utilizador. Com efeito, tais terceiros poderão ser elementos do agregado familiar do utilizador que, porventura, utilizem o mesmo computador para aceder à Internet, como poderão ser outros internautas que detenham com o utilizador subscritor uma relação de confiança e de amizade e que, até, partilhem serviços intermediários²⁷⁹, enfim, toda uma panóplia de situações diferenciáveis e fáctica e tecnicamente impossíveis de serem individualizadas e concretizadas. Assim, não é possível descortinar qualquer vontade do prestador de serviços em proteger tais terceiros. Por outro lado, cai também por terra a utilização desta figura no âmbito da responsabilidade civil por conteúdos ilícitos colocados e difundidos na Internet se atentarmos no facto de a necessidade do interesse do terceiro ser “substancialmente coincidente ou concordante com o do credor da prestação”²⁸⁰, o que também é essencial à aplicabilidade do contrato de protecção para terceiros. Atendendo à

Responsabilidade Civil? – O problema da imputação de danos causados a terceiros por auditores de Sociedades, pp. 88 ss.

²⁷⁵ Assim, JORGE SINDE MONTEIRO, *op. cit.*, p. 520.

²⁷⁶ Exemplos clássicos desta figura, aprofundados com grande êxito na doutrina alemã, como salienta CARNEIRO DA FRADA, *Uma “Terceira via”...*, p. 89, são os contratos de arrendamento (impõe certos deveres de protecção do senhorio face ao agregado familiar do arrendatário) ou o contrato de transporte (os deveres de protecção não cuidam apenas do credor do transporte mas também de eventuais acompanhantes).

²⁷⁷ Vide CARNEIRO DA FRADA, *Uma “Terceira Via”...*, p. 91.

²⁷⁸ Isto é, terá contornos de responsabilidade obrigacional e extraobrigacional. Vide SINDE MONTEIRO, *Responsabilidade por Conselhos...*, p. 522 e n. 241.e CARNEIRO DA FRADA, *Uma “Terceira Via”...*, p. 90 ss.

²⁷⁹ Pense-se, por exemplo, nas redes sociais, ou na co-autoria de um determinado blogue.

²⁸⁰ Neste sentido, CARNEIRO DA FRADA, *Uma “terceira via”...*, p. 92.

diversidade de situações, não poderemos assegurar a existência deste interesse coincidente entre todos os potenciais terceiros próximos do utilizador subscritor.

14.4 Conclusão

Assim, pelo que acabámos de expor, a responsabilidade civil obrigacional dos prestadores de serviços intermediários em rede pelos conteúdos ilícitos colocados e difundidos na Internet pelos seus utilizadores terá reduzida importância prática, uma vez que, na maioria das situações potencialmente ilícitas não nos encontramos perante a violação do contrato de prestação de serviços realizado ou de qualquer um dos deveres de protecção que a ele subjazem. Ressalva feita para os casos em que o utilizador parte no contrato é lesado na sua propriedade, *maxime*, através da danificação do seu *hardware* por força de um vírus, onde concorra na causa da lesão, além da colocação e difusão do conteúdo ilícito, a falta de diligência exigível a um prestador intermediário, dentro dos limites impostos pelo artigo 12.º do RJCE, no sentido da utilização de meios técnicos susceptíveis de evitar a lesão e desde que tal prevenção do risco se encontre no âmbito das práticas costumeiras do sector de actividade do prestador.

15. Balanço do sistema acolhido: A primazia da eficiência do comércio electrónico sobre a tutela efectiva do lesado

Do que resultou exposto do presente capítulo, torna-se evidente que o caminho traçado pelos legisladores estadunidense e comunitário foi no sentido da instauração de um “escudo de defesa” dos prestadores de serviços intermediários face à responsabilidade, *in casu*, civil por conteúdos ilícitos colocados *online* por terceiros.

Como referimos, sempre se discutiu, e discute-se, relativamente aos actos ilícitos perpetrados na rede, quem haveria de sofrer o maior risco: se os lesados que sofriam os danos; se os intermediários que, mesmo que inconscientemente, ajudavam a causar o dano ou a potenciá-lo. O legislador comunitário, na senda do que já tinha sido defendido nos E.U.A., optou por atribuir o maior risco aos lesados, na medida em que contemplou um regime que, como vimos, beneficia o prestador de serviços intermediários, ao estabelecer uma série de isenções de responsabilidade, bem como ao incumbir ao lesado o ónus da prova dos requisitos

que permitem afastar o regime de isenção da responsabilidade dos intermediários, o que, em termos práticos, será bastante difícil de efectivar.

O objectivo foi, por isso, o de potenciar a eficiência e o desenvolvimento do comércio electrónico face à tutela efectiva do lesado. O legislador comunitário assume-o claramente, quando no considerando 40 da DCE refere que: “As divergências actuais ou futuras, entre as legislações e jurisprudências nacionais no domínio da responsabilidade dos prestadores de serviços agindo na qualidade de intermediários, impedem o bom funcionamento do mercado interno, perturbando particularmente o desenvolvimento dos serviços transfronteiriços e produzindo distorções de concorrência. (...)”. A DCE, no considerando 41, também refere que “A presente directiva estabelece um justo equilíbrio entre os diferentes interesses em jogo e consagra princípios em que se podem basear os acordos e normas da indústria.”

Quanto a este segundo ponto, é certo que, nos primórdios da implementação e aplicação da DCE, as possibilidades técnicas de controlo de conteúdos e o número de utilizadores que colocavam conteúdos em rede ainda eram diminutas. No entanto, com o advento da *web 2.0*, cujo crescimento é cada vez maior e onde se assiste à criação e propagação de conteúdos gerados por utilizadores a cada segundo, bem como a grandes proveitos económicos por parte dos intermediários que alojam e difundem esses conteúdos, alguns Estados, bem como alguma jurisprudência e doutrina, têm defendido novas medidas, mais efectivas, de prevenção e repressão dos conteúdos ilícitos na rede, a incidir quer sobre os utilizadores finais, quer sobre os intermediários. Estudaremos brevemente algumas delas, assim como analisaremos a sua (in)viabilidade face ao regime vigente.

CAPÍTULO IV

AS NOVAS TENDÊNCIAS FACE AO REGIME VIGENTE, NO ARQUÉTIPO DA WEB 2.0

16. A exclusão do regime de isenção da responsabilidade com base na ausência da neutralidade típica da actividade de intermediação de serviços *online*

16.1. Termos em que se verifica: alguns casos jurisprudenciais

Conforme referido no ponto anterior, desde a implementação da DCE nos diversos Estados-Membros vimos assistindo a um aumento extraordinário de *sites* compostos por conteúdos gerados por utilizadores, assim como a um incrível sucesso da *web 2.0*, o que proporciona aos utilizadores uma sensação de liberdade como nunca antes se assistiu, bem como proveitos económicos substanciais para os prestadores de serviços intermediários²⁸¹.

Também como já referido, a contratação de serviços da *web 2.0* é tendencialmente gratuita, sendo que os prestadores de serviços intermediários adquirem proveitos económicos através da publicidade que alojam nas várias páginas dos seus *sites*. No entanto, as receitas publicitárias adquiridas são proporcionais ao número de utilizadores que visualizam as páginas e que aí colocam conteúdos, pelo que existe um interesse dos prestadores de serviços intermediários no incentivo à colocação de conteúdos nas páginas disponibilizadas. Assim, poder-se-ia dizer que o lucro que os prestadores de serviços intermediários obtêm com os serviços da *web 2.0* disponibilizados encontra-se proporcionalmente ligado ao encorajamento que estes fazem aos seus utilizadores para a publicação e partilha dos seus conteúdos.

Mais, o extraordinário crescimento deste tipo de *sites*²⁸² torna difícil a manutenção da ideia-base de que os únicos fornecedores de conteúdos são os próprios utilizadores dos serviços e os respectivos prestadores simples intermediários de serviços.

Por outro lado, o sistema de *notice and take down* norte-americano acolhido na DCE e, consequentemente, no RJCE, não raras vezes se torna inútil para a prevenção total do dano, apenas servindo para a sua limitação, na medida em que, como referido *supra*²⁸³, pressupõe uma actuação *a posteriori* do intermediário no sentido da remoção do conteúdo ilícito após a

²⁸¹ Neste sentido *vide* LILIAN EDWARDS, op. cit., p. 67.

²⁸² Veja-se, a título de exemplo, que no final de 2010 o *Facebook* tinha atingido já quinhentos milhões de utilizadores.

²⁸³ *Vide* p. 75.

sua colocação em rede. Tal limitação assume particular crítica no seio das associações de direitos de autor, na medida em que a colocação em rede de um conteúdo pirateado, mesmo que por breves momentos, pode levar à consumação total do dano, na medida em que será muito difícil a completa apreensão do material ilegal e respectivas cópias, quando o mesmo seja colocado em rede.

A título de exemplo, refira-se o serviço de leilões *online* do prestador de serviços intermediários *Ebay*, que tem sido alvo de vários processos judiciais, principalmente por sociedades comerciais detentoras dos direitos de marcas de moda como a *Tiffany* ou a *Louis Vuitton*, devido à existência de leilões de produtos falsificados. O *Ebay* possui uma política de utilização²⁸⁴ do seu serviço que evidencia claramente que a venda de material falsificado é absolutamente proibida. No entanto, a efectivação dessa política é, na maior parte dos casos, ineficaz, na medida em que o *Ebay* se assume como um intermediário de serviços e, por essa razão, apenas eventualmente toma alguma medida após a denúncia da existência do material ilícito por algum interessado, o que, por vezes, poderá chegar tarde demais. Por outro lado, o *Ebay* recebe uma percentagem sobre o preço final de cada objecto que é colocado no *site* para leilão. Existe, assim, um benefício económico directo para o *Ebay* em virtude da venda de conteúdos colocados por terceiros (utilizadores).

A existência efectiva desse benefício económico directo poderá colocar em causa a neutralidade do intermediário de serviços – essencial para que caia na noção de “prestador de serviços intermediários” constante do n.º 5 do artigo 4.º do RJCE – na medida em que o intermediário já será parte interessada na colocação de conteúdos *online* e, por essa razão, a disponibilização de serviços já poderá não ser independente da geração da própria informação transmitida. E, por isso, já poderá ser exigível ao prestador de serviços que actue activa e preventivamente na remoção de conteúdos ilegais que sejam colocados e/ou difundidos na rede pelos serviços que disponibiliza. A este respeito refira-se uma decisão jurisprudencial francesa, relativamente a um litígio de 2008 que opôs a *Louis Vuitton Moët Hennessy (LVMH)* e o *Ebay*, devido a leilões de produtos falsificados que decorriam no *site* do prestador de serviços²⁸⁵. O *Tribunal de Commerce* de Paris entendeu que o *Ebay* era responsável por não ter conseguido impedir a venda do material falsificado através dos seus serviços, tendo afastado a actividade do *Ebay* do âmbito de aplicação das isenções de

²⁸⁴ Cujo conteúdo pode ser visualizado em <http://pages.ebay.com/help/policies/overview.html> (última visualização em 27.07.2011).

²⁸⁵ *Louis Vuitton Moët Hennessy (LVMH) vs. Ebay* (2008). Para mais desenvolvimentos, vide LILIAN EDWARDS, *op. cit.*, p. 68 ss.

responsabilidade previstas na lei francesa de transposição da DCE, considerando que a sua actividade, por não ser neutra em relação aos conteúdos colocados e transmitidos pelos seus serviços, se encontrava fora do conceito de prestação intermediária de serviços.

De igual forma, já a 22 de Junho de 2007, o *Tribunal de Grande Instance* de Paris havia condenado o *Myspace*²⁸⁶, um fornecedor de alojamento principal, por alojar no seu *site* vários desenhos de um conhecido humorista francês, cujo *upload* era feito por terceiros utilizadores do serviço disponibilizado pelo prestador e sem a prévia autorização do humorista, que detinha direitos de autor sobre os desenhos. O tribunal considerou que o *Myspace* não se cingia à mera actividade de intermediação, na medida em que apresenta uma estrutura de apresentação por quadros (janelas) cuja visualização se permite a qualquer utilizador do serviço e, por outro lado, coloca anúncios nos vários quadros, que surgem por cada visita que se faça aos mesmos, levando a que, no caso em concreto, o prestador de serviço obtivesse um benefício económico considerável com o alojamento daqueles desenhos. Assim, o tribunal considerou que o *Myspace* estaria afastado do regime de isenção, sendo-lhe aplicável o regime geral da responsabilidade civil, comparando a sua situação à de um *editor*.

As duas decisões jurisprudenciais citadas, ambas providas de França²⁸⁷, evidenciam uma linha de pensamento que, embora não seja maioritária²⁸⁸, considera os serviços proporcionados pela *web 2.0* mais complexos do que os simples serviços de intermediação. Tal posição resulta não só do exponencial crescimento da utilização destes serviços – para o bem e para o mal – mas também do potencial lucrativo que os mesmos acarretam para o prestador dos serviços. É este potencial lucrativo, ou, melhor dizendo, o benefício económico que os prestadores de serviços *online* recebem dos conteúdos colocados pelos utilizadores que coloca a neutralidade, típica e característica da actividade de intermediação de serviços, em causa e, consequentemente, leva a que o regime de isenção de responsabilidade seja afastado *tout court*, pelo menos nos casos jurisprudenciais vindos de referir.

²⁸⁶ Jean Yves L. dit Lafesse vs. Myspace (2007).

²⁸⁷ Curiosamente o Estado Europeu cuja posição nos primórdios do debate sobre a responsabilidade dos prestadores de serviços intermediários em linha mais tendia para a sua responsabilização.

²⁸⁸ Veja-se que a maioria das decisões jurisprudenciais nesta matéria se pronunciam a favor dos prestadores de serviços intermediários e, portanto, contra a sua responsabilização. Vide, a título de exemplo, *Tiffany(NJ) Inc v. Ebay* (2008), julgado a 14 de Julho de 2008 pelo Tribunal Distrital de Nova Iorque, que considerou que o *Ebay* não poderia ser responsabilizado com base no conhecimento geral de que vendas de materiais contrafeitos poderiam ocorrer no seu *site* e que, ao invés, deveria recair sobre o detentor da marca, a *Tiffany*, o ónus de “fiscalizar” o bom uso da mesma. Refira-se ainda que o tribunal constatou que a lei norte-americana poderia ser insuficiente para a tutela conveniente das marcas no mundo digital, mas, não obstante, face ao direito constituído, a decisão não poderia ir em sentido diferente da efectivamente tomada. Para mais desenvolvimentos vide LILIAN EDWARDS, *op. cit.*, pp. 68 ss.

16.2. Análise crítica

Como aponta LILIAN EDWARDS²⁸⁹, não existe ainda uma base jurisprudencial sólida relativamente a litígios relacionados com a *web 2.0*, não por falta de fundamentos para haver responsabilidade (vimos *supra*²⁹⁰ alguns deles), mas pelo facto de a maioria dos litígios emergentes acabarem por não chegar a julgamento, terminando o processo com uma transacção entre as partes.

Assim, toda a análise crítica que se faça a esta nova tendência de exclusão do regime da isenção de responsabilidade civil com fundamento na falta de neutralidade do intermediário de serviços carecerá sempre de ser confrontada com novos casos jurisprudenciais que entretanto surjam nos ordenamentos jurídicos.

De todo o modo, poderemos desde já adiantar que o afastamento do regime de isenção de responsabilidade para o prestador de serviços intermediários implica sempre de uma análise casuística, nomeadamente quanto ao concreto benefício económico que o prestador obteve com a colocação e difusão do conteúdo e a concreta actuação que teve para obter esse benefício. Não bastará, em nosso entender, para afastar o regime da isenção, que o prestador de serviços intermediários em rede tenha obtido um qualquer benefício económico por força da veiculação pelos seus sistemas de um conteúdo ilícito. É necessário que o benefício seja directamente atribuível ao conteúdo ilícito e que para isso tenha contribuído o próprio prestador (mas, quanto a este último ponto, já bastará uma contribuição indirecta, em nosso entender).

Nestes termos, torna-se necessário diferenciar as situações hipotéticas que poderão existir. Desde logo, analisando o modelo de negócio do *Ebay supra* descrito, constatamos que o prestador de serviços disponibiliza um espaço no seu servidor para que utilizadores coloquem anúncios de venda de objectos através de um leilão que, por sua vez, decorre *online*, durante um prazo definido pelo utilizador e mediante uma base de licitação também por este definida. O *Ebay*, embora não cobre nenhum montante prévio para a utilização do serviço, acaba por cobrar uma comissão sobre o preço de venda do produto obtido no leilão, comissão essa variável consoante o valor em causa. Neste caso, é claro que as comissões cobradas, relativas à venda de produtos falsificados e, por isso, ilegais, traduzem um benefício directo para o *Ebay*. É também claro que existe uma actuação concreta do prestador para

²⁸⁹ *Op. cit.*, p. 73.

²⁹⁰ *Vide* Cap. III.

obtenção desse benefício, que, *in casu*, é a cobrança da referida comissão. Tal modelo de financiamento do serviço extravasa, no nosso entender, o modo de financiamento típico de serviços da *web 2.0*, o que afasta, a nosso ver, o *Ebay* da noção de prestador de serviços intermediários. Ao actuar desta forma, o *Ebay* não age como simples intermediário mas, outrossim, como auxiliar do fornecedor de conteúdos, pelo que o regime de isenção de responsabilidade deve ser liminarmente afastado, sendo de aplicar desde logo o regime geral da responsabilidade civil.

Mas, e o que dizer dos casos em que o benefício económico é retirado da existência de anúncios publicitários nas várias páginas de um determinado *site* de CGU disponibilizado por um prestador de serviços de alojamento? Nestes casos, a solução não será tão líquida. Isto porque, muito embora os serviços típicos da *web 2.0* se distanciem um pouco dos serviços intermediários “tradicionais”, na medida em que assentam o seu modelo de negócio na prestação de serviços gratuita para os seus utilizadores, obtendo receitas económicas por via da publicidade, sendo que os ganhos são maiores quantos mais visualizações um determinado conteúdo for alvo, a verdade é que o modelo de negócio utilizado constitui uma natural consequência da evolução da democraticidade da Internet. Assim, os ganhos com publicidade derivados do número de visualizações que um determinado conteúdo teve não podem significar, só por si, benefício económico directo, de modo a excluir a actividade dos prestadores do regime de isenção de responsabilidade. Caso contrário, estar-se-ia automaticamente a contrariar a tendência evolutiva da Internet e a colocar um ónus demasiado gravoso sobre o comércio electrónico, mesmo que em benefício da tutela dos lesados, o que contrariaria os princípios que subjazem à DCE²⁹¹ e, poderemos dizer mais, afecta irremediavelmente os direitos fundamentais da liberdade de expressão e de informação.

Em resumo, a exploração económica dos serviços *online* através do recurso a publicidade é, em abstracto, susceptível de integrar o conceito da actividade de prestação intermediária de serviços.

Em concreto caberá determinar se o benefício económico resultante da publicidade extravasa, ou não, o carácter neutral de tratamento da informação necessária para se aplicar o regime de isenção da responsabilidade. Para tal, torna-se necessário demonstrar o nexo de

²⁹¹ *Vide*, em concreto, o considerando n.º 1 da DCE, que refere: “O desenvolvimento dos serviços da Sociedade da Informação no espaço sem fronteiras internas é essencial para eliminar as barreiras que dividem os povos europeus.”

causalidade entre o benefício económico e o conteúdo ilícito. JANE C. GINSBURG²⁹² refere-nos dois exemplos que permitem perceber os vários tipos de relação do benefício económico com o conteúdo ilícito: num dos exemplos, o prestador de serviços pode aceitar um modelo de publicidade em que é colocado um anúncio em específico junto de um determinado conteúdo e cujo proveito financeiro aumenta à medida que aumenta o número de visualizações daquele conteúdo; no outro exemplo, o prestador de serviços coloca publicidade aleatória em todo o seu *site* e o proveito financeiro que aquele obtém encontra-se ligado não à popularidade de um determinado conteúdo em particular, mas sim à popularidade do *site* em geral.

Assim, no primeiro exemplo haverá uma mais estreita ligação entre o conteúdo ilícito e o benefício económico obtido através da publicidade, já que o benefício cresce em proporção ao aumento das visualizações do conteúdo em causa, o que poderá levar um juiz a considerar afastado o regime de isenção de responsabilidade. No segundo exemplo, o nexo de causalidade é mais remoto, na medida em que caberá demonstrar em juízo que a popularidade do *site* do prestador de serviços cresceu graças à existência do conteúdo ilícito e que este foi causa exclusiva, ou, no limite, crucial para aquele crescimento.

Pelo exposto, se não temos dúvidas de que a cobrança de comissões ou outro tipo de pagamentos incidentes sobre conteúdos ilícitos em concreto constituem, para todos os efeitos, causa de exclusão do regime de isenção de responsabilidade civil previsto no RJCE, já os benefícios advenientes de receitas publicitárias necessitarão de ser ponderados caso a caso, não só pelas diferentes modalidades que a receita publicitária pode revestir, mas também pelo facto deste modelo de financiamento ser característica essencial para a manutenção dos serviços da *web 2.0*.

17. A obrigação de monitorização *a priori* de conteúdos. A colocação de filtros.

17.1. Termos em que se verifica. O exemplo belga.

Como vimos²⁹³, actualmente o regime legal vigente não prevê a imposição aos prestadores de serviços intermediários de uma obrigação geral de controlo sobre os conteúdos transmitidos e difundidos através dos seus serviços. Ao invés, apenas é previsto para os

²⁹² *Op. cit.*, pp. 238 ss.

²⁹³ *Supra*, pp. 81 ss.

intermediários de alojamento principal a obrigação de retirada dos conteúdos manifestamente ilícitos e apenas após o conhecimento de que os mesmos se encontram alojados nos seus servidores²⁹⁴. Ou seja, apenas lhes é imposto uma retirada de conteúdos *post factum*.

Não obstante o regime legal vigente, os grupos de potenciais lesados, *maxime* as associações de defesa de direitos de autor, entre outros, continuam a lutar pela imposição de uma obrigação de controlo *a priori* dos conteúdos que se pretendem que sejam alojados e/ou postos em circulação através dos serviços disponibilizados pelos prestadores intermediários.

Por outro lado, os próprios Estados começam a ficar tentados a impor aos prestadores de serviços intermediários a obrigação de filtrar a informação transmitida, a fim de combater o terrorismo ou de remover da rede conteúdos divulgados cobertos pelo segredo de estado²⁹⁵.

O avanço tecnológico a que hoje se assiste também potencia a reabordagem à capacidade efectiva do prestador de serviços intermediários poder exercer um controlo *a priori*, ou, pelo menos, um controlo em tempo real dos conteúdos que são colocados e difundidos através dos seus serviços. Exemplo deste avanço tecnológico é o crescente desenvolvimento de ferramentas de *Deep Packet Inspection* (DPI) – isto é, ferramentas tecnológicas que permitem a um prestador de serviços intermediários não só identificar o tipo de conteúdos que é colocado e transmitido nos seus servidores como visualizar o próprio conteúdo em si.

A existência destas ferramentas e a sua utilização por parte dos prestadores de serviços intermediários poderá ser defensável, na medida em que torna possível o controle de conteúdos de maneira mais eficaz que o sistema de *notice and take down* legalmente instituído. No entanto, por outro lado, torna-se altamente invasivo da privacidade nas telecomunicações, ainda para mais tendo em conta que estas ferramentas podem ser utilizadas para a visualização de conteúdos transmitidos através de *e-mails*, o que é, em tudo, semelhante à abertura de correspondência privada alheia²⁹⁶.

Assim, encontramos-nos perante um conflito entre dois bens jurídicos distintos: por um lado a segurança e as boas práticas na Internet e, por outro lado, a confidencialidade das

²⁹⁴ Vide *supra* pp. 85 ss.

²⁹⁵ A este respeito refira-se, uma vez mais, o fenómeno da divulgação de mais de 250 mil telegramas enviados de várias embaixadas norte-americanas pela organização *Wikileaks*. O prestador de serviços intermediário de alojamento do *site* da *Wikileaks*, a empresa *EveryDNS.net*, acabou por encerrar o *site*, alegando que o mesmo estava a ser alvo de vários ataques informáticos que poderiam danificar não só o *site* da *Wikileaks* mas também outros *sites* de outros clientes do prestador. Claro que, à parte desta versão oficial, muitos defendem que o prestador de serviços actuou subordinado ao governo norte-americano, encerrando o *site* devido ao manifesto incómodo que a divulgação dos referidos telegramas, muitos de carácter confidencial, trazia para os E.U.A.

²⁹⁶ Sobre os benefícios e malefícios da monitorização de conteúdos por parte dos prestadores de serviços intermediários vide, por todos, PAUL OHM, “The rise and fall of invasive ISP surveillance”, in *Colorado Law*.

informações transmitidas, a privacidade nas telecomunicações. Pergunta-se então até que ponto será razoável permitir o uso de tecnologias de monitorização por parte dos prestadores de serviços intermediários e até que ponto será razoável exigir dos mesmos a adopção desses mecanismos?

PAUL OHM²⁹⁷ refere cinco razões que poderão justificar o recurso às ferramentas de monitorização por parte dos prestadores de serviços intermediários. Desde logo, é de referir a identificação de protocolos TCP/IP, na medida em que é através destes protocolos que o prestador consegue saber qual o destinatário que solicitou o serviço a fim de o reenviar para este. Além desta primeira razão, advêm mais quatro razões, sendo elas: a filtragem de *spam*; a identificação e eliminação de vírus; a necessidade de assegurar a segurança da rede do prestador de serviços face a actos provocados por terceiros, por exemplo, próprios utilizadores do serviço; por fim, a necessidade de melhoramento da largura de banda da rede do prestador de serviços, com o fim de descongestionamento da mesma.

Se, para a filtragem de *spam*, a identificação de vírus e o melhoramento da largura de banda, as ferramentas de DPI aplicáveis podem reduzir-se ao seu âmbito mínimo, no sentido de actuarem automaticamente e com o mínimo de informação retirada do conteúdo que é inspeccionado (pense-se, por exemplo, relativamente à filtragem de *spam* numa conta de correio electrónico, a utilização de programas que memorizam determinadas “palavras chave” que, caso apareçam no “assunto” de uma determinada mensagem electrónica, leva a que a mesma seja rapidamente eliminada e/ou remetida para uma área reservada às mensagens de *spam*), o mesmo já poderá não ocorrer relativamente à necessidade de assegurar a segurança na rede do prestador de serviços contra actos provocados por terceiros²⁹⁸. Neste último caso, porque se encontra ligado intimamente à actuação humana e não meramente à tecnologia informática – como sucede nos restantes casos – é impossível prever como ocorrerá a divulgação do conteúdo ilícito. Assim, para estes casos, poderão ser exigidos mecanismos de monitorização e filtragem de conteúdos mais incidentes no conteúdo da informação em causa, o que obviamente conflitua com a privacidade das comunicações electrónicas. Poderá tal monitorização ser imposta?

A este respeito terá de se referir, por revestir particular importância e actualidade para o assunto que agora abordamos, a decisão do *Tribunal de Première Instance* de Bruxelas de 29

²⁹⁷ *Op. cit.*, pp. 54 ss.

²⁹⁸ Ou, para casos mais complexos de mensagens de *spam* ou vírus electrónicos (pense-se, por exemplo, na difusão de um vírus através de e-mail em que, por cada difusão efectuada pelo *hacker*, a mensagem que o transporta altera automaticamente).

de Junho de 2007²⁹⁹, respeitante a um litígio (ainda não resolvido) entre a *SABAM*, uma associação belga de gestão de direitos de autor e a *Scarlet*, uma empresa belga prestadora de serviços intermediários *online*.

A *SABAM* interpôs a acção em referência, pedindo que o tribunal condenasse a *Scarlet* a colocar filtros no seu serviço de *peer-to-peer* (P2P), de modo a controlar *a priori* o *upload* e *download* ilegal de conteúdos de autores pertencentes à *SABAM* e protegidos pelo Direito de Autor. Para tanto, alegou, entre outras razões, que actualmente a tecnologia existente já permitia à *Scarlet* colocar filtros detectores de conteúdos colocados na sua rede e que violassem direitos de autor.

Por sua vez, a *Scarlet* alegou que a imposição daquela obrigação violava o disposto no artigo 15.º da DCE e o correspondente *article 21* da *Loi 2003-03-11/32*, de 11 de Março de 2003, que obriga os Estados-membros a não imporem aos prestadores de serviços intermediários uma obrigação geral de vigilância sobre as informações que os mesmos transmitem ou armazenam³⁰⁰. Mais advertiu que a instalação de filtros levaria a que a actividade de simples transporte da *Scarlet* ficasse excluída do regime de isenção respectivo, na medida em que este, para ser aplicável, implicaria que o prestador não seleccionasse os conteúdos a transmitir. Por outro lado, defendeu que a instalação de filtros permanentes e sistemáticos violaria direitos fundamentais, nomeadamente os direitos à privacidade, à confidencialidade das comunicações e à liberdade de expressão e de informação. Por fim, requereu que, numa eventual condenação, fosse a *SABAM* que suportasse os custos da implementação das novas medidas técnicas de filtragem, uma vez que era esta a parte interessada na sua colocação e, por isso, deveria a mesma suportar os custos daquela implementação.

Para o efeito de saber até que ponto existiam meios técnicos que permitissem a filtragem de conteúdos no sistema da *Scarlet*, o tribunal incumbiu um perito de analisar a situação, a fim de providenciar aos autos o relatório da sua investigação.

No relatório que apresentou, o perito identificou onze soluções que seriam tecnicamente eficientes para a filtragem de conteúdos P2P, embora tenha entendido que dessas onze soluções apenas sete poderiam ser aplicáveis à rede da *Scarlet*. E dessas sete, apenas uma,

²⁹⁹ Tradução em língua inglesa da sentença disponível em MADY, BOURROUILLOU & HUGHES, “CAELJ Translation Series #001”, in *Cardoso Arts & Entertainment Journal*, n.º 25.

³⁰⁰ Não obstante, o *article 21* da lei belga diverge sensivelmente do normativo comunitário, na medida em que prevê que tal obrigação não impede as autoridades judiciais competentes de imporem uma obrigação de vigilância, desde que esta se reporte a um caso em específico, seja temporária, e esteja prevista na lei, o que, na verdade, consubstancia uma concretização da liberdade deixada pela DCE no seu considerando n.º 48.

denominada *Audible Magic*, servia o propósito de identificar os conteúdos de música protegidos por direitos de autor no tráfego P2P, na medida em que as restantes se tratavam de ferramentas que permitiam a gestão do tráfego de informação, não tendo como objectivo distinguir as informações transmitidas consoante o seu conteúdo.

Não obstante o perito identificar uma medida susceptível de alcançar o fim almejado pela SABAM, de imediato advertiu que a eficácia da implementação da *Audible Magic* não ultrapassaria os dois ou três anos, na medida em que se assiste ao crescimento do uso de ficheiros encriptados nestes tipos de aplicações. O perito adiantou também que a *Audible Magic* se encontrava principalmente pensada para o uso na área da educação e não para a intermediação de serviços *online* onde o volume de tráfego é exponencialmente maior. Tal facto levaria a um grave aumento dos custos da actividade pela sua aplicação (v.g., o intermediário seria obrigado a comprar várias licenças do produto de modo a conseguir aplicá-lo em toda a sua rede) o que, quando comparado com o tempo de duração em que se previa a efectividade da filtragem (dois a três anos), levou o perito a concluir pela ineficiência desta medida para o objectivo almejado pela SABAM – a filtragem permanente e *a priori* dos conteúdos que circulam pela rede da *Scarlet*.

Não obstante as considerações feitas pelo perito, o tribunal belga teve um entendimento diferente, advogando que a aplicação do sistema do *Audible Magic* não só era possível no caso em análise como era necessária. O tribunal considerou que a SABAM provou que o mecanismo da *Audible Magic* já era utilizado pelo prestador de serviços intermediários *Myspace* que, por sua vez, possui uma das plataformas mais utilizadas para a troca de conteúdos entre os utilizadores de Internet. Por outro lado, a própria *Microsoft* já se encontrava a implementar a ferramenta e, por fim, a SABAM também indicou um estudo de 2005 relativo a um prestador de serviços intermediários asiático que havia implementado a *Audible Magic* e cuja conclusão demonstrava que a tecnologia podia ser usada para identificar e filtrar os conteúdos protegidos pelo Direito de Autor que circulassem na rede do intermediário.

O entendimento do perito foi assim afastado pelo tribunal, não só pelas provas careadas para os autos pela SABAM, bem como pelo facto de o perito não ter dado elementos fácticos que permitissem perceber até que ponto é que o uso de ficheiros encriptados na rede da *Scarlet* seria assim tão frequente, tendo em conta que, tal como a SABAM alertou, o sistema de P2P, pela sua própria natureza aberta a todos os demais utilizadores, implicaria

necessariamente que a maior parte dos seus conteúdos estivesse acessível a todos e, por maioria de razão, não se encontrasse encriptada.

Por fim, o tribunal também considerou que os custos associados à implementação desta medida não eram tão elevados como inicialmente esperado, na medida em que, de acordo com a averiguação feita, os custos não ultrapassariam os 0,50 € por mês e por utilizador.

Relativamente à incompatibilidade da imposição da filtragem à *Scarlet* em face do regime da DCE, e respectiva transposição belga, o tribunal argumentou que tal não era incompatível com a não imposição de uma obrigação geral de vigilância, na medida em que esta disposição legal, apenas é aplicável no âmbito do regime da responsabilidade dos prestadores de serviços intermediários e, no que ao caso respeitava, apenas estava em discussão a imposição de uma medida de monitorização de conteúdos e não a apreciação da responsabilidade da *Scarlet* pela ausência de implementação dessa medida.

O tribunal vai mais longe: citando o considerando n.º 40 da DCE, no sentido que não é impedido aos Estados-Membros imporem as medidas técnicas de protecção e identificação que sejam possíveis à luz da tecnologia existente; referindo que a colocação de filtros não consubstancia uma obrigação geral de vigilância, na medida em que as ferramentas utilizadas se limitam a bloquear e a filtrar certas informações vinculadas pelo sistema da *Scarlet* e essa filtragem é feita de forma automática e sem necessidade de o intermediário intervir na filtragem.

Por esta última razão, também o tribunal refere que a imposição de filtros não exclui a *Scarlet* da isenção de responsabilidade pelas actividades de mero transporte, uma vez que tal só sucederia se a *Scarlet* seleccionasse propositadamente os conteúdos que queria transmitir. Com a filtragem automática a isenção mantém-se, mesmo para conteúdos que, embora ilegais, consigam ultrapassar os filtros. E, refere ainda o tribunal, mesmo que por mera hipótese se considerasse que a *Scarlet* ficaria excluída da isenção, ainda seria necessário provar a efectiva responsabilidade do prestador, isto é, que a transmissão do conteúdo lhe era imputável, a título de dolo ou negligência.

Por fim, o tribunal refuta a alegada violação do direito à privacidade que tal medida de filtragem poderia acarretar, na medida em que a imposição deste tipo de filtros em nada difere do *software* já existente de *anti-vírus* ou *anti-spam*, que, por serem meramente técnicos, não envolvem qualquer processo de identificação de informações pessoais, mas apenas a seriação de determinados conteúdos com base em palavras-chave previamente definidas. Relativamente à hipotética violação do sigilo na correspondência ou da violação da liberdade

de expressão e de informação, o tribunal apenas argumenta que não logra visualizar tal violação e que a *Scarlet*, por sua vez, não trouxe qualquer facto para os autos que provasse que essa violação pudesse ocorrer.

Pelo exposto, o tribunal condenou a *Scarlet* a, no prazo de 6 meses, implementar as medidas de filtragem de acordo com a ferramenta do *Audible Magic*, e estabeleceu uma sanção pecuniária compulsória no valor de € 2.500,00, por cada dia de atraso naquela implementação. Mais referiu que os custos da implementação correriam por conta da *Scarlet*, por aplicação analógica do artigo 1248 do código civil belga.

Da decisão a *Scarlet* recorreu para a *Cour d'appel* de Bruxelas que, por sua vez, suscitou a questão prévia de saber se a decisão de primeira instância está de acordo com o ordenamento jurídico comunitário, em particular com a Carta dos Direitos Fundamentais da União Europeia, procedendo ao reenvio dos autos para o Tribunal de Justiça da União Europeia.

No momento em que escrevemos estas páginas ainda se aguarda pela decisão do Tribunal de Justiça da União Europeia, cujo sentido poderá constituir um precedente importante, caso este se pronuncie a favor da decisão tomada pelo tribunal de primeira instância belga. No entanto, a 14 de Abril de 2011, ficou já conhecido o parecer do advogado-geral, M. Cruz Villalón, que se pronunciou no sentido da revogação da decisão belga, por entender que a imposição deste tipo de filtros, mais do que contrariar a obrigação de não vigilância³⁰¹, configura uma limitação do direito ao respeito do segredo das comunicações e do direito à protecção dos dados pessoais, bem como aponta a desproporcionalidade na restrição efectuada à liberdade de informação face à protecção dos direitos de autor das obras dos associados da *SABAM* que a medida visa atingir. A sustentar tal entendimento, refere o advogado-geral o facto de a imposição decidida pela justiça belga ser uma filtragem definitiva e não temporária e o facto do próprio sistema de filtragem em si não assegurar, com suficiente precisão, a filtragem adequada dos conteúdos. O advogado-geral adianta também que uma limitação destes direitos apenas seria possível caso existisse uma base legal nacional específica, clara e previsível para tal, o que não sucede no presente caso³⁰².

³⁰¹ Na verdade, o advogado-geral parece nem abordar a questão quanto a esta hipotética violação.

³⁰² Vide comunicado de imprensa n.º 37/11.

17.2 Análise crítica

O problema da monitorização dos conteúdos por parte dos prestadores de serviços intermediários é, e sempre será, uma questão controversa no seio do debate a que está subjacente a responsabilidade civil pelos conteúdos colocados e difundidos na Internet. Em particular, são claras as forças em confronto: por um lado, a maior protecção que a monitorização de conteúdos poderá dar face aos potenciais lesados; por outro lado, a limitação de direitos fundamentais como o direito à protecção dos dados pessoais, da privacidade das comunicações electrónicas e, ainda, da liberdade de expressão e de informação.

Actualmente, é um facto, como vimos, que a monitorização e filtragem são possíveis. Contudo, tais ferramentas apenas poderão ser eficazes para retirar da rede conteúdos que possam ser identificados automaticamente, como vírus ou obras protegidas pelo Direito de Autor. Para o combate a conteúdos que dependam de uma avaliação prévia humana da ilicitude do conteúdo, como ofensas ao bom nome, ou violação do direito à imagem de uma pessoa, as técnicas de monitorização e filtragem existentes já não serão eficientes. Nestes segundos casos, a filtragem e monitorização automáticas não deixarão ainda de ser algo apenas presente no imaginário futurista. E, mesmo quanto ao primeiro grupo de casos, não é possível às tecnologias actuais diferenciar, no caso de conteúdos protegidos pelo Direito de Autor, quais os conteúdos realmente ilegais ou aqueles que estão a ser utilizados com autorização do seu autor nem mesmo se tal utilização cabe dentro dos pressupostos da utilização livre prevista no n.º2 do artigo 75.º do CDADC. A tudo isto acresce a possibilidade de conteúdos ilícitos, mesmo com as medidas de filtragem implementadas, conseguirem passar sem serem detectados, nomeadamente através de mecanismos de encriptação de dados.

Por outro lado, a utilização deste tipo de medidas, principalmente a DPI, pode implicar graves atentados aos direitos fundamentais dos internautas. Como já referimos *supra*³⁰³, a vontade de tornar os prestadores de serviços intermediários “polícias” das suas próprias redes pode trazer efeitos muito negativos para vários direitos fundamentais, *maxime* a liberdade de expressão e de informação. Quando tais medidas de filtragem e monitorização não forem completamente eficazes, ainda mais se poderá colocar em questão a razoabilidade da imposição de tais medidas em face das limitações a direitos fundamentais que tal imposição acarreta.

³⁰³ Vide pp.104 ss.

Como salienta LILIAN EDWARDS, “No futuro, parece que a questão não será se a filtragem por intermediários é ou não possível, mas sim se será obrigatória, que grau de precisão será exigido, que custos podem razoavelmente ser impostos e que trade-offs em termos de liberdade de expressão, privacidade, processo legal e restrição de acesso ao conhecimento são aceitáveis”³⁰⁴.

A nosso ver, actualmente, as medidas existentes de filtragem e monitorização ainda não apresentam uma segurança e fiabilidade suficientes que nos faça defender a sua imposição aos intermediários *tout court*. Não obstante, assiste-se à preocupação dos prestadores de serviços intermediários colocarem filtros, principalmente para protecção de direitos de autor, como são disso exemplo o caso já referido do *Myspace*, bem como a ferramenta *Claim your content*, desenvolvida pela *Google* para ser utilizada no *Youtube*³⁰⁵.

Assim, em nosso entender, dependendo da evolução tecnológica que as medidas de filtragem possam ter nos próximos tempos, poderemos eventualmente estar perante a quebra de um dos grandes pilares em que assenta a isenção de responsabilidade dos prestadores de serviços intermediários – a falta de meios técnicos economicamente sustentáveis para o controlo dos conteúdos que circulem nas redes dos prestadores de serviços intermediários.

E será que, actualmente, existe margem legal para a imposição aos prestadores de serviços intermediários das medidas de monitorização e de filtragem conhecidas? Entendemos que não. Ao contrário do defendido pelo *Tribunal de Première Instance* de Bruxelas, entendemos que a imposição de uma obrigação de monitorização e filtragem permanentes dos conteúdos viola o disposto no artigo 15.º da DCE. Isto porque, apesar de tal norma se reputar ao âmbito da responsabilidade dos prestadores de serviços intermediários, em nosso entender, a imposição de um dever de filtragem e monitorização de conteúdos geral e abstracto, como sucedeu *in casu* com a sentença belga, acaba por determinar uma obrigação geral de vigilância. O que significará que, se tal sistema de filtragem falhar, o prestador acabará por ser responsabilizado, uma vez que incumpriu a obrigação estabelecida pelo tribunal, ou, caso contrário, estar-se-á perante uma “condenação sem sanção”. A tentativa de imposição de deveres gerais de vigilância, ainda que apenas mediante condenações *a posteriori* que imponham a adopção desses comportamentos, viola o regime comunitário. Tanto assim é que

³⁰⁴ *Op. cit.*, p. 85.

³⁰⁵ Embora esta ferramenta não seja de cariz geral e abstracto como a *Audible Magic*, pois exige a prévia indicação do titular dos direitos de autor das obras que deverão ser filtradas, sendo uma espécie de medida intermédia entre a filtragem proporcionada pela *Audible Magic* e o sistema de *notice and take down*. Para mais desenvolvimentos *vide* ERIK VALGAEREN e NICOLAS ROLAND, *op. cit.*, pp. 221 ss.

a DCE prevê a imposição de deveres de vigilância apenas em casos específicos³⁰⁶. A imposição de um dever de filtragem de conteúdos *tout court*, como sucedeu *in casu* com o tribunal de Bruxelas, viola, em nosso entender, o regime comunitário. Prevemos, por isso, que o Tribunal de Justiça da União Europeia acabe por revogar a referida decisão, não só com base na violação de direitos fundamentais comunitários, como apontou o advogado-geral, mas também com base na violação, ainda que indirecta, do artigo 15.º da DCE.

18. Reincidências sobre a responsabilidade do dono da coisa. O exemplo paradigmático da Lei HADOPI

18.1. Termos em que se verifica

Tem-se assistido, actualmente, a uma produção legislativa no sentido de aumentar a segurança da Internet e o combate a conteúdos ilícitos colocados e difundidos *online* que passa, *in extremis*, pelo corte de acesso à Internet dos utilizadores que pratiquem actos ilícitos na rede.

Neste sentido foi pioneira a *Loi favorisant la diffusion et la protection de la création sur Internet*, vulgarmente denominada de Lei HADOPI³⁰⁷, que procedeu à alteração do *Code de la propriété intellectuelle* francês. O termo HADOPI decorre das siglas da *Haute Autorité pour la Diffusion des Oeuvres et la Protection des Droits sur Internet*, uma autoridade pública independente que foi criada pela lei em causa, destinada a supervisionar o cumprimento da mesma³⁰⁸.

A Lei HADOPI, como o próprio nome indica, visa uma reacção por parte do Estado, *in casu*, da Alta Autoridade para a Difusão de Obras e Protecção de Direitos na Internet, às violações de direitos de autor que são perpetradas na Internet.

Para tal, a lei adopta um procedimento baseado numa “resposta gradual” de três passos, internacionalmente conhecido como “*three strikes and you’re out*”³⁰⁹. A HADOPI, mediante queixa prévia relacionada com violação de direitos de autor que lhe seja reportada, notifica o

³⁰⁶ Cfr. Considerando n.º 47 da DCE.

³⁰⁷ *Loi n.º 2009-699* de 12 de Junho de 2009. O grande promotor da referida Lei foi, curiosamente, o presidente executivo da FNAC, Dennis Olivenne.

³⁰⁸ Para um desenvolvimento mais aprofundado do papel da Lei HADOPI no ordenamento jurídico francês *vide* SÓNIA QUEIROZ VAZ, “A nova legislação francesa sobre obrigações dos ISP’s quanto à retenção dos dados dos infractores e o respeito dos direitos de propriedade intelectual”, in *Lusíada.Direito*, pp. 237 ss.

³⁰⁹ Neste sentido *vide* LILIAN EDWARDS, *op. cit.*, p. 82.

prestador intermediário de serviços de acesso para fornecer as informações que detém sobre o titular da conta de acesso à rede que foi utilizada para perpetuar o acto ilícito³¹⁰. Após a obtenção dessa informação, a HADOPI envia uma notificação por *e-mail* para o titular da referida conta em causa, reportando a situação que foi detectada³¹¹. Caso seja descoberta uma nova infracção através da mesma conta de acesso, no prazo de 6 meses desde o envio da notificação por *e-mail*, esta é repetida, mas, desta vez, através de envio por carta registada com aviso de recepção para o domicílio do titular da conta. Se, no prazo de um ano a contar desde a segunda notificação, for cometida uma nova infracção, a HADOPI instaura um procedimento criminal contra o titular da conta de acesso à rede em causa, podendo o tribunal impor como pena acessória a suspensão do acesso do titular à Internet por um período que poderá durar desde 3 meses a 1 ano. O prestador intermediário que celebrou o contrato de acesso à Internet com o titular condenado é obrigado a cortar esse acesso durante o período de interdição definido pelo tribunal, apesar de manter o direito às prestações pecuniárias devidas como se continuasse a prestar o serviço de acesso à rede. Por outro lado, durante a duração da interdição, nenhum outro prestador intermediário pode celebrar um novo contrato de acesso à Internet com o titular condenado. O titular da conta fica, assim, numa situação de “*isolamento virtual*”.

Assume particular destaque, no entanto, o facto de a Lei HADOPI impor ao titular da conta de acesso – geralmente também o proprietário do(s) computador(es) utilizado(s) para aceder à Internet com aquela conta - um dever de vigilância sobre a utilização da Internet através desse mesmo acesso, cabendo a este, na eventualidade da detecção de qualquer violação de direitos de autor perpetuada através do seu acesso, demonstrar que não foi ele o prevaricador. A lei ainda vai mais longe no sentido de entender que tal presunção de culpa apenas se encontra afastada no caso de colocação de *filtros anti-pirataria*, cujo modelo é previamente aprovado pela HADOPI. Poderemos assim dizer que a Lei HADOPI vem dar um “novo fôlego” à responsabilidade do dono da coisa no âmbito da Internet³¹². A rematar, diga-

³¹⁰ A exigência de um Estado-membro impor ao prestador intermediário a obrigação do armazenar nas suas bases de dados as informações necessárias à identificação do autor do conteúdo ilícito foi prevista pela DCE, nos termos do n.º 2 do artigo 15.º, *in fine*. Em França essa obrigação surgiu precisamente com a Lei HADOPI. Em Portugal, como já vimos, tal obrigação resulta do disposto no artigo 13.º alínea b) do RJCE.

³¹¹ Até ao presente momento consta já terem sido notificados cerca de quatrocentos mil utilizadores.

³¹² *Vide supra*, p. 69, n. 158.

se que tal presunção de culpa vigora não só ao nível da responsabilidade civil, mas também ao nível da responsabilidade criminal³¹³.

Como facilmente se compreende, a Lei HADOPI não foi, e não é, uma lei isenta de polémica. A polémica resultou logo de uma decisão do *Conseil Constitutionnel* de 10 de Junho de 2009³¹⁴, que, entre outras normas, declarou inconstitucional a norma primitiva da Lei HADOPI que previa que o corte de acesso à rede pudesse ser decretado pela própria HADOPI, sem intervenção do tribunal. O tribunal constitucional francês considerou que o legislador não podia permitir que uma autoridade administrativa, em defesa do Direito de Autor, limitasse o direito de acesso à Internet por parte dos cidadãos, na medida em que tal direito consubstanciava um corolário da liberdade de expressão e pensamento, constitucionalmente protegida. Assim, o *Conseil Constitutionnel* entendeu que a restrição imposta pela Lei HADOPI apenas poderia ser decretada por um tribunal judicial, o que acabou por ser implementado no texto actualmente em vigor. Os defensores deste entendimento referem ainda que a existência e utilização de serviços de comunicação ao público em linha, proporcionados pela Internet, é fulcral para a participação na vida democrática e partilha de pensamentos e opiniões e que tal apenas é possível com o acesso à Internet a todos e sem barreiras³¹⁵.

A Lei HADOPI também é atacada devido à utilização de dados pessoais pela autoridade administrativa sem a prévia autorização da Comissão de Protecção de Dados francesa. Os prestadores de serviços intermediários, por outro lado, alegam que, com a Lei HADOPI, passam a ter novos custos - com a adaptação das suas infra-estruturas à necessidade de conservação dos dados de cada utilizador e dos pedidos de colaboração por parte da autoridade administrativa - custos esses que aparentam ser excessivos para o fim que se visa atingir.

Porém a principal crítica que se faz à Lei HADOPI prende-se, em suma, com a aparente desproporcionalidade entre o fim que visa – a protecção de direitos de autor e direitos conexos – e as medidas utilizadas para a prossecução desse fim – a imposição de um dever de vigilância sobre o titular da conta de acesso à Internet e a possibilidade de aplicação de uma pena acessória consubstanciada no corte desse acesso. Poderemos dizer que a Lei HADOPI

³¹³ Não incumbe neste estudo abordar a “bondade” da aplicabilidade da presunção de culpa no campo criminal. Não deixaremos, no entanto, de referir que tal facto nos parece um completo “absurdo jurídico” e, ademais, conflituante com a garantia constitucional do *in dubio pro reo*.

³¹⁴ *Décision n° 2009-580 DC du Conseil Constitutionnel* (2009).

³¹⁵ Vide SÓNIA QUEIROZ VAZ, *op. cit.*, pp. 239 ss.

configura uma ampla restrição de direitos fundamentais do Homem, como a liberdade de expressão e de informação.

Nem todas as vozes são contra a Lei HADOPI. Facilmente se compreende que a Lei HADOPI tenha reunido muitos defensores no seio das associações de gestão colectiva de direitos de autor³¹⁶. Desde logo porque, através do seu sistema protectoral, consubstanciado na imposição de deveres de vigilância e na consagração de punições fortes e efectivas, consegue determinadamente reduzir os actos de pirataria levados a cabo na Internet, principalmente através da redução do número de *downloads* ilegais efectuados por utilizadores.

Não obstante as polémicas existentes, parece que, por enquanto, a Lei HADOPI veio para ficar. Na verdade, um estudo publicado pela Universidade de Rennes, pelo *Mole Armoricaín de Recherche sur la Sociéte de l'Information et les Usages d'Internet*³¹⁷, demonstra que 15% dos internautas que utilizavam serviços P2P – serviço que é actualmente o mais utilizado para *downloads* ilegais – antes da implementação da Lei HADOPI deixaram de os utilizar após a sua implementação. De igual forma, 25% dos que ainda continuam a utilizar os serviços P2P, depois da implementação da Lei HADOPI alteraram as suas práticas de modo a não utilizar aqueles serviços para fins ilícitos. A Lei HADOPI tem, assim, demonstrado resultados no fim que visa atingir, apesar da aparente desconformidade com os princípios e direitos fundamentais nacionais e da União Europeia.

O conteúdo da Lei HADOPI não é único no seio dos ordenamentos jurídicos da Europa. Espanha também procedeu a uma série de alterações à *Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico*^{318 319}, através daquela que ficou conhecida como a *Lei Sinde*³²⁰. A *Lei Sinde*, contudo, não visa “atacar” o titular da conta de acesso responsável pela actuação ilícita, mas sim o serviço que permite tal actuação. Por outras palavras, a autoridade administrativa criada pela *Lei Sinde* pode determinar a interrupção da prestação do

³¹⁶ E de empresas multinacionais cujo fim de actividade é a comercialização de obras artísticas *latu sensu*, como, por exemplo, a FNAC.

³¹⁷ Vide SYLVAIN DEJEAN, THIERRY PÉNARD e RAPHAËL SUIRE, *Une première évaluation des effets de la loi HADOPI sur les pratiques des Internauts français*.

³¹⁸ E antes de Espanha, também a Suécia seguiu os passos da Lei HADOPI, tendo publicado a chamada Lei IPRED.

³¹⁹ A já referida *Ley 34/2002 de 11 de Júlio*.

³²⁰ A lei ficou assim apelidada em virtude do nome da Ministra da Cultura Angeles Gonzalez Sinde, que foi a pessoa responsável pela redacção da proposta de lei.

serviço ou intimar o prestador de serviços para retirar os conteúdos ilícitos da rede, mas já não tem poderes para solicitar ao prestador de serviço de acesso que corte o acesso à Internet a um determinado utilizador.

Em Portugal, embora não exista, actualmente, qualquer regulamentação legal em termos iguais ou semelhantes aos da Lei HADOPI³²¹, o debate sobre este tipo de medidas já se começa a sentir, nomeadamente quanto à possibilidade de utilização de um software denominado *honeypot*, que consiste numa forma de simular um determinado ficheiro ilegal que é, posteriormente, carregado numa rede P2P, de modo a identificar quem descarrega esse conteúdo³²².

18.2. Análise crítica

A utilização deste tipo de medidas, embora envolta em grande polémica, como constatamos, acaba por ganhar grandes adeptos no grupo dos defensores da propriedade intelectual e dos grupos económicos de comercialização de produtos autorais, pois atinge directamente a grande causa de violação dos direitos de autor: a pirataria informática.

Não obstante, colocamos sérias reservas aos modelos propostos, principalmente ao modelo proposto pela Lei HADOPI, pela desproporcionalidade que, em nossa opinião, existe entre o fim que visa atingir e os mecanismos legais adoptados.

As razões destas reservas prendem-se logo no que diz respeito ao dever de vigilância imposto ao dono da coisa, *in casu* o titular da conta de acesso à Internet, e igualmente proprietário do computador utilizado para o acesso. Desde logo, a identificação fornecida pelos prestadores de serviços intermediários (ou por qualquer outra entidade) pode não ser necessariamente coincidente com a identificação do verdadeiro infractor. Isto porque, como já constatámos, actualmente é impossível conseguir identificar uma concreta pessoa que acede à Internet, mas apenas o computador que ela usa para aceder à Internet, mediante o número de IP³²³.

³²¹ Apenas existe a previsão da obrigação dos prestadores de serviços intermediários alojarem, pelo prazo de um ano, a fim de poderem ser utilizados pelas autoridades judiciais competentes na investigação de crimes graves, nos termos do disposto na Lei n.º 32/2008 de 17 de Julho. Não obstante, o tribunal pode impor medidas injuntivas como a cessação de determinado tipo de actividades, nos termos das disposições penais previstas no CDADC, que poderão, em certa medida, ser aplicadas analogicamente ao “mundo virtual”.

³²² Disso nos dá conta FERNANDA GALDO ROLÓN, “Ley Sinde y la lucha contra la piratería”, in *Economía Ibérica*, p. 54.

³²³ Vide *supra*, pp. 68 ss.

Ora, existem várias formas de dissimular o verdadeiro IP, sendo uma delas, o IP *spoofing*, a que já aludimos *supra*³²⁴. Ora, caso tal aconteça e o autor do acto ilícito usurpe um IP alheio, de acordo com a Lei HADOPI, a pessoa que irá ser notificada do acto ilícito será o terceiro detentor da conta de acesso a que o IP usurpado se encontra associado e não o próprio infractor. Na verdade, terá esse terceiro de demonstrar em tribunal que o acto ilícito não proveio verdadeiramente do seu IP e que este foi utilizado para fins ilegítimos. Imagine-se como é que esse terceiro, com os conhecimentos mínimos de informática que provavelmente terá, conseguirá reunir as provas suficientes para ilidir a presunção gravosa que sobre ele incide?

E como aceitar minimamente tal dever de vigilância no caso de *ciber-cafés*, ou de bibliotecas ou até de faculdades, onde os vários computadores existentes com ligação à Internet são utilizados por várias pessoas em cada dia? Será que, também aqui, os proprietários dos *ciber-cafés*, os bibliotecários ou os directores de faculdade estarão incumbidos da obrigação de monitorizar os conteúdos a que os cidadãos acedem através dos seus computadores? A verdade é que a Lei HADOPI não confere excepções.

Aquela presunção será afastada apenas quando, e se, o titular da conta de acesso instalar *filtros anti-pirataria*, mas não poderão ser quaisquer filtros, apenas os que estejam certificados pela própria HADOPI. Parece-nos que esta solução, sob o manto da nobreza da defesa dos direitos de autor, procura na verdade estabelecer quase que uma “taxa” – que beneficiará as “felizes” empresas cujos filtros sejam certificados pela HADOPI – na medida em que os “bons pais de família”, procurando precaver-se, rapidamente irão adquirir tais filtros. Já os habituais prevaricadores não o irão fazer, optando por investir em melhores programas de *spoofing*, por exemplo. E, ademais, os filtros, como já referido³²⁵, serão pouco efectivos quanto a conteúdos difundidos de forma encriptada.

A presunção de culpa do detentor da coisa imposta pela HADOPI parece-nos, assim, desproporcional e injusta face às falibilidades que tal sistema acarreta quando aplicável à realidade digital que é a Internet.

Por consequência, a possibilidade de aplicação de uma sanção acessória de corte de acesso à Internet sem prova positiva de que o titular da conta de acesso identificado é, na realidade, o infractor, é contrário à Carta dos Direitos Fundamentais da União Europeia. O corte de acesso à Internet implica uma clara e excessiva limitação do direito de acesso à

³²⁴ Vide *supra*, pp. 68 ss.

³²⁵ Vide *supra*, pp. 127 ss.

Internet que, embora não prevista expressamente na Carta de Direitos Fundamentais da União Europeia e, a nível do nosso ordenamento jurídico interno, na Constituição da República Portuguesa, é um corolário do direito à liberdade de expressão e de informação. Pelo que, por mais pragmatismo que tal medida sancionatória possa acarretar para o fim que visa atingir, julgamos que, no estado da tecnologia existente, não é legítimo a um tribunal judicial a aplicação de tal sanção apenas com base numa presunção legal de culpa.

Quanto à obrigação de os prestadores de serviços intermediários armazenarem dados pessoais sobre os seus utilizadores, nomeadamente os dados de IP, entendemos que tal não implica uma violação da reserva da intimidade da vida privada, desde que cumpridas as disposições legais relativas à protecção de dados comunitárias e de cada Estado-Membro³²⁶.

19. O Tratado ACTA

19.1 Termos em que se verifica

Muito recentemente foi assinado um tratado internacional destinado à harmonização internacional relativa à protecção dos direitos de propriedade intelectual. As negociações do *Anti-Counterfeiting Trade Agreement*, vulgarmente designado por ACTA, iniciaram-se em Junho de 2008, tendo os Estados signatários³²⁷ concluído e assinado o texto final no dia 15 de Novembro de 2010.

O ACTA prevê no seu capítulo II uma série de disposições que os Estados signatários terão de aplicar no seu ordenamento jurídico, de forma a aumentar a protecção dos direitos de propriedade intelectual. No âmbito do nosso estudo, assume particular relevância a secção 2, que diz respeito às providências a levar a cabo no âmbito do Direito Civil e a secção 5, relativa às providências a levar a cabo no âmbito do ambiente digital.

A secção 2 refere, em termos gerais, a necessidade de os Estados signatários preverem, nos respectivos ordenamentos jurídicos, a possibilidade de os lesados interpirem junto das autoridades judiciais competentes medidas cautelares de prevenção de danos causados pelo

³²⁶ Por exemplo, em Portugal, todo e qualquer tratamento de dados pessoais carece da autorização prévia da Comissão Nacional de Protecção de Dados, nos termos do disposto na alínea b), do n.º1, do artigo 23.º da Lei n.º 67/98 de 26 de Outubro.

³²⁷ São eles a Alemanha, Austrália, Áustria, Bélgica, Bulgária, Canadá, Chipre, Coreia, Dinamarca, Eslováquia, Eslovénia, Espanha, Estados Unidos da América, Estónia, Finlândia, França, Grécia, Holanda, Hungria, Irlanda, Itália, Japão, Letónia, Luxemburgo, Malta, Marrocos, México, Nova Zelândia, Polónia, Portugal, Reino Unido, República Checa, Roménia, Singapura, Suécia e Suíça. A União Europeia no seu conjunto também fez parte dos signatários do tratado.

uso indevido das obras protegidas³²⁸ – inclusive a possibilidade de utilização de providências cautelares *inaudita altera parte* – bem como a previsão de uma indemnização adequada a compensar os danos causados pela violação de direitos de propriedade intelectual, nomeadamente através do estabelecimento de uma presunção de um valor mínimo para determinar a indemnização que seja suficiente para compensar o lesado dos danos causados.

Por sua vez, a secção 5 refere medidas particulares à protecção dos direitos de propriedade intelectual no mundo tecno-digital. Desde logo, faz alusão ao facto de as medidas previstas na secção 2 (bem como na secção 4 – referente ao âmbito do Direito Penal) terem também de ser aplicáveis no mundo digital.

De destacar ainda, no âmbito da referida secção 5, os pontos 4 e 5. O ponto 4 refere a obrigatoriedade de os Estados signatários implementarem um sistema que permita às autoridades competentes ordenar aos prestadores de serviços intermediários em rede a disponibilização célere de informações sobre os seus utilizadores cuja conta se encontra a ser utilizada para fins ilegais. O ponto n.º5 impõe aos Estados signatários que promovam a protecção legal adequada para que seja possível a adopção de medidas técnicas que possam ser utilizadas pelos autores da(s) obra(s) de modo a restringir ou impossibilitar o uso não autorizado das mesmas.

O Tratado ACTA promove assim uma linha comum de harmonização da protecção dos direitos de propriedade intelectual no mundo digital, no que ao nosso estudo diz respeito, ditando directrizes genéricas para que os Estados signatários promovam tal protecção, tendo em conta as particularidades do ordenamento jurídico de cada Estado.

19.2. Análise Crítica

É ainda cedo para nos podermos pronunciar sobre a bondade das directrizes apontadas pelo ACTA, bem como sobre a sua importância prática quando for efectivamente implementado pelos Estados signatários³²⁹. O ACTA promove uma série de indicações que os Estados signatários necessitam de prover, indicações essas que manifestam as preocupações que se começam a sentir no dealbar deste novo paradigma da *web 2.0*.

Muitos críticos do ACTA apontam que este tratado, pelo seu carácter geral e abstracto, dá uma espécie de “carta branca” aos seus signatários para colocarem toda a espécie de

³²⁸ Vide, em particular, o artigo 12.º do ACTA.

³²⁹ Não obstante a sua assinatura a 15 de Novembro de 2010, o ACTA apenas entrará em vigor 30 dias após o depósito do sexto instrumento de ratificação por parte dos Estados signatários, o que ainda não sucedeu.

mecanismos de protecção dos direitos de propriedade intelectual, bem como para ignorarem certos direitos e liberdades fundamentais, tais como a liberdade de expressão ou o direito à privacidade, o que, pelo menos no caso da União Europeia, tem um valor de relevo.

Entendemos que o ACTA não dá esta “carta branca” que os críticos referem. Com efeito, as suas disposições prevêm que o Estado signatário actue, não só em conformidade com as indicações do tratado, mas também em conformidade com o seu ordenamento jurídico, *maxime*, os seus direitos fundamentais. Além do mais, o ACTA prevê expressamente no artigo 6.º – um artigo que enuncia os princípios gerais a ter em conta nas medidas de protecção – que as medidas a adoptar deverão ser aplicadas de forma a não criar barreiras às transacções legais de obras protegidas, bem como se deverá ter em conta na sua aplicação o critério de proporcionalidade entre a ilegalidade cometida, o interesse de terceiros (p.e. prestadores de serviços intermediários), as medidas aplicáveis e as sanções previstas³³⁰.

O ACTA é, a nosso ver, uma manifestação de princípio e uma tentativa de harmonização supra-comunitária das medidas aptas a proteger direitos de propriedade intelectual. Restará aguardar para saber como se concretizarão tais medidas de protecção, bem como serão as mesmas conciliadas com princípios tão fundamentais como a liberdade de expressão ou o direito à reserva da intimidade da vida privada. Tal concretização, no que toca à União Europeia, uma vez que também ela é signatária do tratado, não deverá trazer substanciais mudanças, na medida em que muitos dos princípios consagrados no ACTA encontram-se plasmados em várias Directivas comunitárias já transpostas³³¹. Na verdade, o ACTA mais parece um documento, celebrado fundamentalmente entre os E.U.A. e os Estados-membros da União Europeia, que visa dar um *standard* mínimo de protecção da propriedade industrial e intelectual – e, conseqüentemente, dos padrões indemnizatórios em caso de violação destes direitos – que, muito provavelmente, se tentará impor a outros Estados, menos proteccionistas nestas matérias, para que se consiga obter uma harmonização verdadeiramente internacional.

Em todo o caso, os próximos desenvolvimentos do que será o ACTA na prática envolverão certamente todos os intervenientes num debate longo e aceso até à sua concretização.

³³⁰ Vide, em particular, ponto 1 e 3 do artigo 6.º.

³³¹ Em particular a DCE e a Directiva n.º 2004/48 do Parlamento Europeu e do Conselho.

20. Caminhos a trilhar?

As novas tendências que vimos a descrever demonstram dois factos.

Por um lado, começamos a assistir a um aumento do poder e influência dos grupos de interesse dos lesados, *maxime*, das associações de gestão colectiva de direitos autorais, face aos grupos de interesse dos prestadores de serviços intermediários online. Na verdade, começamos a assistir a uma preocupação dos Estados em promover uma maior protecção dos direitos de autor face à Internet, da qual a Lei HADOPI é disso um claro exemplo.

Por outro lado, verifica-se uma certa desconformidade do regime jurídico da responsabilidade civil dos prestadores de serviços intermediários face ao panorama evolutivo actual da Internet e, em particular, da *web 2.0*. Como vimos, a preferência pela isenção de responsabilidade dos prestadores intermediários residia em três pilares-chave:

- *A impossibilidade técnica de os prestadores de serviços intermediários exercerem um controlo prévio e efectivo dos conteúdos colocados e difundidos através dos seus serviços;*
- *A neutralidade dos prestadores de serviços intermediários face aos conteúdos colocados por utilizadores e que eram transmitidos pelos seus sistemas;*
- *Por fim, as consequências para o direito de acesso à Internet, para a expansão da mesma e para a eficiência do comércio electrónico que resultariam da não adopção de um sistema de isenção de responsabilidade.*

Estas novas tendências resultam, porém, da constatação de que estes três pilares-chave que justificam a isenção da responsabilidade dos prestadores intermediários perderam muita da sua relevância no paradigma actual da *web 2.0*³³².

Desde logo, constatamos a emergência de tecnologias que permitem a filtragem *a priori* de conteúdos colocados em rede, embora, como referimos *supra*³³³, tais técnicas ainda não tenham atingido o grau adequado a permitir o desempenho de tal função com total eficiência sem ser demasiado intrusiva na confidencialidade das comunicações e na reserva da intimidade da vida privada.

Constatamos ainda que, com os serviços da *web 2.0*, muitas vezes o intermediário, pelo próprio modelo lucrativo que adopta – proveito económico através da publicidade – dinamiza e incentiva a colocação e difusão de conteúdos por parte dos seus utilizadores, potencializando as funcionalidades do seu sistema consoante mais utilizadores coloquem

³³² Neste sentido *vide* LILIAN EDWARDS, *op. cit.*, pp. 84 ss.

³³³ *Vide* pp. 127 ss.

conteúdos no mesmo e, conseqüentemente, adquirindo maiores margens lucrativas. Assim, o argumento usado da neutralidade dos prestadores de serviços intermediários face aos conteúdos que armazenam e/ou transmitem começa a perder grande força. Se não relativamente a todas as actividades de intermediação, pelo menos quanto às actividades de armazenamento principal de conteúdos.

Por fim, actualmente a Internet encontra-se consolidada na sociedade, fazendo já parte do quotidiano, se não de todos, da maior parte dos cidadãos. Os prestadores de serviços intermediários encontram-se plenamente implementados nos vários Estados da União Europeia, à luz do que sucedeu nos E.U.A., pelo que poder-se-á argumentar que a abolição do regime de isenção não abalará a eficiência e a sobrevivência da Internet na União Europeia, como foi defendido na altura da implementação do regime da DCE.

Assim, o advento da *web 2.0* torna necessária, a nosso ver, uma revisão do regime da responsabilidade dos prestadores de serviços intermediários. No entanto, não somos de opinião que, actualmente, seja de afastar liminarmente o sistema de isenção de responsabilidade existente.

Na verdade, apesar da evolução técnica a que vimos assistindo e do novo modelo de negócio dos serviços característicos da *web 2.0*, os prestadores de serviços intermediários não deixaram, a nosso ver, de ser, na maioria dos casos, intermediários. É verdade que, nalgumas situações, como verificámos³³⁴, o benefício económico encontra-se tão directamente ligado ao conteúdo ilícito que não será possível abranger esse serviço na actividade de intermediação³³⁵. Assim, desde logo, julgamos útil, de modo a harmonizar jurisprudência eventualmente divergente quanto a este aspecto, a normativização do conceito de “benefício económico directo” à luz do que sucede no DMCA estadunidense. Depois, caberá ao julgador-intérprete enquadrar a actividade de intermediação concreta à luz desse conceito, de modo a afastá-lo, ou não, do regime de isenção.

Por outro lado, no nosso entender, incumbirá reforçar a tutela do lesado face à imunidade do intermediário. Com efeito, parece-nos razoável que passe a incumbir ao prestador de serviços intermediários a prova dos requisitos para estar abrangido pelo regime de isenção de responsabilidade. Não nos poderemos esquecer que o prestador intermediário é,

³³⁴ Vide *supra* pp. 118 ss.

³³⁵ Tendo como exemplo o *Ebay* e o seu sistema de cobrança de comissões sobre os produtos leiloados no seu *site*.

para todos os efeitos, o proprietário da rede de sistemas informáticos dos seus serviços, bem como o interveniente que em melhor posição se encontra para localizar e remover qualquer conteúdo ilícito que seja colocado ou difundido através dos seus sistemas. Assim, e também atendendo à falência parcial dos pilares que pautaram a criação da isenção de responsabilidade do intermediário, defendemos a previsão de uma presunção de culpa deste, no sentido de lhe incumbir a prova dos requisitos de isenção previstos no regime do RJCE. Não seria, de resto, uma alteração que estaria em contradição com o ordenamento jurídico português, ou mesmo o europeu, na medida em que, com o mesmo fundamento, o legislador previu situações em que o ónus da prova corre por conta do proprietário do objecto – falamos da responsabilidade por danos causados por edifícios, ou até dos danos causados por atravessamento de animais nas auto-estradas³³⁶.

Naturalmente tal inversão do ónus da prova apenas se aplicará à responsabilidade civil dos prestadores de serviços intermediários, pois que a presunção de culpa não pode ser aplicada à responsabilidade criminal, sob pena de violação do princípio constitucionalmente protegido *in dubio pro reu*.

Assim, os intermediários terão a seu cargo o dever de demonstrar que se encontram abrangidos pelo regime de isenção, consoante o tipo de actividade exercida.

Na actividade de simples transporte, terá o intermediário de demonstrar que não tem intervenção no conteúdo das mensagens transmitidas nem na selecção destas ou dos destinatários.

Na actividade de *caching* terá o intermediário de demonstrar que efectua a armazenagem intermediária com o único e exclusivo propósito de tornar mais eficaz e económica a transmissão posterior da informação, a nova solicitação do destinatário. Terá também de demonstrar que efectua a actualização da informação armazenada e utiliza a tecnologia informática de acordo com as regras usuais do sector. Caso a informação deixe de estar disponível na fonte originária, terá o intermediário também de provar que não continua a armazenar aquela informação nos seus servidores.

Nas actividades *supra* referidas, de acordo com a alteração do ónus da prova por nós sugerida, incumbirá apenas ao lesado demonstrar o dano que foi produzido por força do facto do prestador. Demonstrando tais requisitos, incumbirá a estes prestadores demonstrarem que a sua actividade se encontra isenta de responsabilidade civil. Caso não o logrem demonstrar, então serão, em nosso entender, responsáveis civilmente, na medida em que, como

³³⁶ Vide artigo 492.º CC e artigo 12.º da Lei n.º 24/2007 de 18 de Julho.

defendemos *supra*³³⁷, as obrigações presentes na DCE e RJCE são também critérios delimitadores dos requisitos da responsabilidade civil, pelo que a falta de cumprimento das obrigações da DCE e RJCE equivalem ao preenchimento dos requisitos do facto, da ilicitude e da culpa.

No que diz respeito à armazenagem principal e à associação de conteúdos, ao adoptar-se um sistema baseado na presunção de culpa, o prestador intermediário terá de demonstrar que não teve conhecimento da actividade ou informação cuja ilicitude for manifesta ou, caso não o demonstre, terá de provar que retirou ou impossibilitou o acesso à informação ilícita após o conhecimento da mesma. Não obstante, a par desta alteração, deverão também ser delineados, por exemplo em termos semelhantes aos definidos no DMCA, os parâmetros do que constitui uma notificação ao prestador de serviços válida³³⁸ para efeitos de conhecimento do conteúdo ilícito. Assim, caso a notificação enviada ao prestador não cumpra os requisitos que vierem a ser definidos, este poderá afastar a presunção de culpa da sua actuação, demonstrando que a notificação não era válida para que o intermediário pudesse actuar. Desta forma, o agravamento da prova do regime de isenção da responsabilidade civil do intermediário seria colmatado com a segurança jurídica deste saber quais as notificações por parte de terceiros a que deverá atender.

Invertendo assim o ónus da prova julgamos conseguir equilibrar de forma mais equitativa os “pratos da balança”. Por um lado, os eventuais lesados terão mais garantias de se verem ressarcidos dos danos que sofram em virtude dos conteúdos ilícitos que circulem na Internet, por outro lado, um agravamento na responsabilidade civil dos prestadores intermediários como o proposto contrabalançará com os enormes proveitos financeiros que obtêm com os serviços prestados e poderá servir de incentivo para que estes adoptem novas formas mais eficazes de controlo dos conteúdos que circulam nos seus servidores e de identificação dos seus utilizadores. De resto, a *ratio* da presunção de culpa neste âmbito não será diferente, como referimos, da utilizada quanto aos donos de edifícios ou quanto às concessionárias de auto-estradas: enquanto proprietários dos sistemas e das ferramentas utilizadas para a colocação e difusão de conteúdos *online* serão os intermediários quem estará em melhores condições para demonstrar que a sua actividade ainda se insere dentro do âmbito da isenção de responsabilidade, pelo que deverá ser sobre estes que recairá o ónus dessa prova.

³³⁷ Vide pp. 91 ss.

³³⁸ Vide *supra*, pp. 96 ss.

Claro que qualquer alteração que se faça ao nível da normativização da responsabilidade civil dos intermediários, como a sugerida *supra*, carecerá sempre de ser conciliada com todos os Estados-Membros, pelo que terá de ser desencadeada nas instituições comunitárias. Atrevemo-nos, inclusive, a dizer que tal alteração deverá ser sempre concertada com o ordenamento jurídico norte-americano, para uma mais completa harmonização. Falamos não de uma harmonização comunitária, mas, ao invés, de uma harmonização supra-comunitária da responsabilidade civil dos prestadores de serviços intermediários, à semelhança do que já sucedeu com a convenção internacional sobre o cibercrime³³⁹ e com o recente Tratado ACTA.

De igual forma, assumem neste campo suma importância a criação de códigos de conduta, a divulgar por todos os internautas, nomeadamente aquando da subscrição de serviços, naquilo que é comumente designado por *softlaw*. Os códigos de conduta permitem não só advertir os utilizadores para uma sã utilização do serviço, como também adaptar as exigências legais à especificidade do serviço em causa³⁴⁰. A própria DCE incentiva a criação destes códigos de conduta, no seu artigo 16.º.

A par dos códigos de conduta é necessário que a sociedade civil eduque os seus membros para a Sociedade da Informação, no sentido de uma maior consciencialização e auto-responsabilização dos utilizadores pelos seus actos, transmitindo a ideia muitas vezes esquecida nestas matérias de que “o que é ilícito fora da rede também o é dentro dela”³⁴¹.

Por fim, deverá ser incentivada a criação de mecanismos de resolução alternativa de litígios, bem como a criação de tribunais especializados para a resolução de questões relacionadas com responsabilidade civil na Internet, bem como outras questões da Sociedade da Informação.

³³⁹ A convenção internacional sobre o cibercrime, também denominada de Convenção de Budapeste, foi assinada no dia 23 de Novembro de 2001, precisamente em Budapeste, constituindo o seu texto um conjunto de opções legislativas que cada parte signatária teria de adoptar no ordenamento jurídico interno, com vista a uma harmonização da repressão e punição deste fenómeno criminal. Para mais desenvolvimentos *vide* JOEL TIMÓTEO RAMOS PEREIRA, *Compêndio...*, pp. 511 ss. A Convenção sobre o cibercrime, em conjunto com a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, estiveram na origem da recente Lei do Cibercrime – Lei n.º 109/2009 de 15 de Setembro.

³⁴⁰ Neste sentido *vide* MARÍA NÉLIDA TUR FAÚNDEZ, *op. cit.*, pp.159 ss e, também, ALEXANDRE CRUQUENAIRE, *op. cit.*, p. 105.

³⁴¹ De resto, uma ideia que já havíamos defendido no nosso “A responsabilidade civil pelo conteúdo da informação transmitida através dos blogues”, p. 40.

O mecanismo da resolução provisória de litígios consagrado no artigo 18.º RJCE é um bom passo neste sentido e, em teoria, uma ótima alternativa às providências cautelares não especificadas³⁴². No entanto, não parece existir vontade legislativa para o regulamentar, de modo a ser efectivamente implementado.

Actualmente também se encontra a ser implementado um Centro de Informação, Mediação e Arbitragem do Comércio Electrónico (CIMACE): no entanto, parece não servir para a resolução de litígios relacionados com a colocação de conteúdos na Internet³⁴³.

Deverão também ser implementados tribunais especializados em matérias da Sociedade da Informação, na medida em que para uma correcta resolução do litígio caberá, não raras vezes, conhecer com detalhe as circunstâncias técnicas de processamento e circulação da informação, circunstâncias essas que se alteram a um ritmo acelerado, o que implica que o julgador se mantenha sistematicamente actualizado, não apenas em termos jurídicos, mas também em termos técnicos, de conhecimento do meio onde irá, posteriormente, aplicar o Direito. Tal acompanhamento não será viável num tribunal genérico, onde o juiz tenha a seu cargo processos de várias matérias diferentes, mas apenas num tribunal especializado, cuja competência seja individualizada e focalizada nas matérias da Sociedade da Informação. A criação do Tribunal de Propriedade Intelectual, embora não criado com este propósito particular, constitui já um passo nesse sentido, atendendo à inevitável importância desta área do Direito na Sociedade da Informação.

Em suma, certo é que, tal como salienta LILIAN EDWARDS³⁴⁴, “uma linha clara de irresponsabilidade dos intermediários pelo conteúdo fornecido por terceiros (...) não pode continuar a ser sustentada. Com ou sem intervenção legislativa supranacional, estamos a verificar uma evolução para um novo sistema europeu, dirigido pelo Direito feito pelos tribunais europeus, leis nacionais e regulamentação da própria indústria (...)”³⁴⁵.

Com efeito, ainda não é certo qual o rumo que a União Europeia irá tomar em relação à responsabilidade civil dos intermediários face ao paradigma da *web 2.0* e às manifestações “protectorais” dos vários Estados-membros através das novas tendências indicadas *supra*. A

³⁴² Cfr. artigo 381.º do Código de Processo Civil.

³⁴³ Com efeito, de acordo com o Protocolo entre as partes signatárias, disponível em <http://www.gral.mj.pt/userfiles/Protocolo%20-%20Assinado.pdf> (consultado em 27.07.2011), o CIMACE é apenas aplicável aos litígios emergentes da interpretação, validade e execução de contratos electrónicos e litígios emergentes da infracção de normas de protecção dos direitos do consumidor.

³⁴⁴ *Op. cit.*, pp. 87 ss.

³⁴⁵ Tradução livre feita por nós.

União Europeia parece querer adiar, pelo maior tempo possível, um novo debate sobre a responsabilidade civil dos intermediários, porventura já antevendo a polémica que tal debate irá causar.

Quanto a nós, sugerimos algumas linhas de acção que, salvo melhor opinião em contrário, são aptas a serem tomadas tendo em conta os dados conhecidos e existentes. Restará aguardar para ver se, numa eventual revisão da DCE, a opção do legislador comunitário será, ou não, a mesma que aqui trilhámos.

CONCLUSÕES

Necessário se torna concluir. Ao longo destas páginas procurámos evidenciar os problemas jurídicos que se suscitam no âmbito da aplicação da dogmática comum da responsabilidade civil à realidade fáctica da Internet, em particular no que respeita aos conteúdos gerados pelos utilizadores.

Da presente investigação resultou que o sistema dogmático comum da responsabilidade civil ainda é, em teoria, capaz de responder ao ressarcimento de danos ocorridos numa esfera jurídica diferente daquela que os causou. Os “odres velhos” da responsabilidade civil encontram-se ainda robustos para receber e conservar o “vinho novo” da Internet³⁴⁶.

Mas, como constatámos, a efectivação prática da responsabilidade civil do autor do conteúdo ilícito colocado e difundido na rede possui duas grandes dificuldades, que derivam da natureza digital da Internet: por um lado, o carácter transnacional desta e consequente dificuldade na determinação da ilicitude de um determinado conteúdo à luz do ordenamento jurídico potencialmente aplicável; por outro lado, o uso da Internet sob o anonimato, potenciado pelas suas características essencialmente digitais.

Assim, seguindo as pisadas dos ordenamentos jurídicos norte-americanos e comunitários, procurou-se seguir outro caminho, no sentido de responsabilizar civilmente os prestadores de serviços intermediários que providenciam os mecanismos técnicos aptos a difundir os conteúdos (ilícitos ou não) dos respectivos utilizadores. No entanto, conforme apurámos, tal responsabilização teria de actuar em moldes muito restritos, quer pela própria natureza dos intermediários enquanto meros “mensageiros” dos conteúdos, quer pela impossibilidade técnica de controlo ou filtragem *a priori* dos conteúdos por eles transmitidos.

Analisámos o regime jurídico vigente em Portugal, que transpôs a DCE para o nosso ordenamento. O regime estabelece uma série de isenções de responsabilidade para os prestadores de serviços intermediários, consoante a actividade que exerçam. Desenvolvemos ainda alguns pontos críticos desse regime que, de acordo com a letra da lei ambígua, necessitam de concretização doutrinária e jurisprudencial.

Desta análise conseguimos concluir que o legislador comunitário e, consequentemente, o legislador nacional, optaram por consagrar, em termos práticos, um regime de tendencial

³⁴⁶ CARNEIRO DA FRADA, “Vinho novo em odres velhos?..”, p. 31.

“desresponsabilização” da actividade dos prestadores de serviços intermediários, em detrimento da tutela jurídica do lesado.

Não obstante, verificamos que, em plena apoteose da *web 2.0*, alguns dos dogmas em que assentava o regime de isenção de responsabilidade dos intermediários começam a perecer. Decisões jurisprudenciais, embora ainda minoritárias, tendem a afastar tal regime, ou por considerarem as actividades dos prestadores de serviços da *web 2.0* fora do conceito de “intermediação de serviços”, ora por entenderem que, actualmente, a tecnologia informática já permite impor ao prestador a aposição de um sistema de filtragem de conteúdos, ainda que tal imposição apenas possa surgir depois de uma condenação *a posteriori*. Por outro lado, alguns Estados procuram acautelar as expectativas dos lesados, principalmente no campo do Direito de Autor, através da revitalização da responsabilidade do dono da coisa, isto é, do titular da conta de acesso à Internet. Por fim, independentemente do caminho a nível da responsabilidade civil por conteúdos colocados e difundidos na Internet que se tome, parece clara a intenção de, em algumas temáticas, nomeadamente no campo da Propriedade Industrial e Intelectual, se proceder a uma harmonização supra-comunitária de aspectos relativos à responsabilidade civil.

Fizemos a nossa análise crítica das tendências que se verificam actualmente. Entendemos que alguns dos caminhos apontados ainda são demasiado precoces e carecem de sedimentação para serem encarados como alternativas viáveis ao sistema de isenção de responsabilidade dos prestadores de serviços intermediários implementado. De igual forma, temos muitas dúvidas do efectivo sucesso da Lei HADOPI e do ónus que tal lei impõe sobre o titular da conta de acesso à Internet, não obstante acreditarmos que tal modelo será implementado na maioria dos países da União Europeia, devido ao *lobby* das associações de direitos de autor e empresas de comercialização de obras protegidas.

Pela nossa parte, continuamos a considerar que os serviços prestados na *web 2.0*, salvo algumas excepções, continuam a manter a característica de “intermediação”, sendo o novo modelo de financiamento de tais serviços apenas uma consequência inevitável da evolução da Internet e do comércio electrónico. Não obstante, aceitamos que alguns dos pilares-chave, que justificavam a implementação do regime de isenção no início do milénio, perderam muita da sua relevância neste novo paradigma.

Assim, entendemos que deverá ser operada uma mudança no regime vigente, mantendo as cláusulas de isenção da responsabilidade civil do intermediário na sua essência, mas, ao invés, invertendo o ónus da prova, no sentido de incumbir a este a prova de que se encontram preenchidos os requisitos da isenção de responsabilidade civil, tendo em conta que o intermediário, enquanto proprietário da rede de sistemas informáticos dos seus serviços, será, à partida, a parte mais apta a demonstrar os referidos requisitos. De resto, esta presunção de culpa não estará em contradição com outros exemplos semelhantes existentes no ordenamento jurídico português ou comunitário.

Em suma, a responsabilidade civil pelos conteúdos ilícitos colocados e difundidos na Internet não é um assunto encerrado. O paradigma da *web 2.0* e dos conteúdos gerados por utilizadores voltaram a colocar a problemática em cima da mesa.

Este estudo procurou, essencialmente, fornecer uma visão de conjunto dos principais problemas que se suscitam neste âmbito e do “estado actual da arte”, procurando apontar alguns caminhos para o futuro. Esperamos ter dado um contributo oportuno ao debate da responsabilidade civil neste constantemente mutável meio de comunicação e de desenvolvimento das sociedades contemporâneas.

João Fachana

Julho de 2011

BIBLIOGRAFIA

Monografias (por ordem alfabética)

AKESTER, Patrícia – *O Direito de Autor e os desafios da tecnologia digital*. Lisboa: Principia. 2004;

ANTUNES, Henrique Sousa – *Responsabilidade civil dos obrigados à vigilância de pessoa naturalmente incapaz*. Lisboa: Universidade Católica Editora. 2000;

ASCENSÃO, José de Oliveira – “O Direito de Autor e a Internet. Em particular as recentes orientações da Comunidade Europeia”. In *Direito da Sociedade da Informação*. Vol. VII. Coimbra: Coimbra Editora. 2008;

- *Direito Civil: Direito de Autor e Direitos Conexos*. 2ª ed. Coimbra: Coimbra Editora. 2008 (reimpr.);

BRO, Ruth Hill – “Defamation Online”. In SMEDINGHOFF, Thomas J. (ed. lit.) – *Online Law*. EUA: Addison-Wesley Developers Press. 1996;

CARVALHO, Pedro Pitta e Cunha Nunes de, *Omissão e dever de agir em Direito Civil*, Coimbra: Almedina, 1999;

CASIMIRO, Sofia de Vasconcelos – *A Responsabilidade Civil pelo Conteúdo da Informação Transmitida pela Internet*. Coimbra: Almedina. 2000;

CASSANO, Giuseppe – *Diritto dell’ Internet: Il Sistema di tutele della persona*. Milão: Giuffrè Editore. 2005;

CORDEIRO, António Menezes – *Tratado de Direito Civil Português : II – Das Obrigações*. Tomo III. Coimbra: Almedina. 2010;

- *Direito das Obrigações*. 2º Vol. Lisboa: Associação Académica da Faculdade de Direito de Lisboa. 1994;

COSTA, Mário Júlio de Almeida – *Direito das Obrigações*. 12ª ed. Coimbra: Almedina. 2009;

CRUQUENAIRE, Alexandre – “Transposition of the E-commerce directive: some critical comments”. In *Direito da Sociedade da Informação*. Vol. V. Coimbra: Coimbra Editora. 2004;

EDWARDS, Lilian – “The fall and rise of Intermediary Liability Online”. In EDWARDS, Lilian; WAELDE, Charlotte (coord.) – *Law and the Internet*. 3.^a ed. E.U.A.: Hart Publishing. 2009;

FACHANA, João – “A Responsabilidade Civil pelo conteúdo da informação transmitida através de blogs”. In *Jusjournal* (13.05.2010). Disponível em www.jusjournal.pt (consult. em 27.07.2011) ;

FARIA, Jorge Leite Areias Ribeiro de – *Direito das Obrigações*. Vol. I e II. Coimbra: Almedina. 2003 (reimpr.);

FAÚNDEZ, Maria Nélida Tur – “La responsabilidad contractual de los intermediarios electrónicos”. In MÚGICA, Santiago Cavanillas (coord.) *Deberes y responsabilidades de los servidores de acceso y alojamiento: un análisis multidisciplinar*. Granada: Editorial Comares. 2005;

FRADA, Manuel A. Carneiro da – *Direito Civil – Responsabilidade Civil: O método do caso*. Coimbra:Almedina. 2010 (reimpr.);

- *Teoria da Confiança e Responsabilidade Civil*. Coimbra:Almedina.2007;

- ““Vinho Novo em Odres Velhos”? A responsabilidade civil das “operadoras de Internet” e a doutrina comum da imputação de danos”. In *Direito da Sociedade da Informação*. Vol. II. Coimbra: Coimbra Editora. 2001;

- *Uma “terceira via” no Direito da Responsabilidade Civil?: o problema da imputação de danos causados a terceiros por auditores de sociedades*. Coimbra: Almedina. 1997;

- *Contrato e deveres de protecção*. Coimbra. 1994. Tese de mestrado;

GALLEGO, Mónica López-Morús (coord.); ROS, Rafael Mateu de; URÍBARRI, José Manuel Villar *et. allia* – *Derecho de Internet – La Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico*. Navarra: Editorial Aranzadi. 2003;

GEORGE, Carlisle; SCERRI, Jackie - “Web 2.0 and User-Generated Content: legal challenges in the new frontier”. In *Journal of Information, Law and Technology*. N.º 2. 2007. Disponível em <http://go.warwick.ac.uk/jilt/> (consult. em 27.07.2011);

GINSBURG, Jane C. – “Whose tube? Liability risks and limitations of copyright-dependent technology entrepreneurs”. In STROWEL, Alain; TRIAILLE, Jean – Paul (coord.) – *Google et les nouveaux services en ligne: impact sur l’économie du contenu et questions de propriété intellectuelle*. Bruxelas: Lacier. 2008;

HOEREN, Thomas – “Liability for online services in Germany”. In *German Law Journal*, vol. 10, n.º5, 2009. Disponível em <http://www.germanlawjournal.com/> (consult. em 27.07.2011);

LEITÃO, Luís Manuel Teles de Menezes – *Direito das Obrigações*. Vol. I. 9ª ed. Coimbra: Almedina. 2010;

- “A distribuição de mensagens de correio electrónico indesejadas (SPAM)”. In *Direito da Sociedade da Informação*. Vol. IV. Coimbra: Coimbra Editora. 2003;

- “A Responsabilidade Civil na Internet”. In *Direito da Sociedade da Informação*. Vol. III. Coimbra: Coimbra Editora. 2002;

LÓPEZ, Valentín Carrascosa; SOTO, Carlos Ferreyros; AGUILAR, Audilio Gonzáles – *Los contratos en la sociedad de la información – formularios de contratos informáticos e internet*. Granada: Editorial Comares. 2004;

MACHADO, João Baptista, - *Introdução ao Direito e ao Discurso Legitimador*. Coimbra: Almedina. 2002;

MAGNI, Sabrina; SPLOIDORO, Marco Saverio - “La Responsabilità degli Operatori in Internet: Profili Interni Internazionali”. In *Diritto dell’Informazione e dell’Informatica*. ano XIII. n.º1. 1991.

MARQUES, Garcia; MARTINS, Lourenço – *Direito da Informática*. 2ª ed. Coimbra: Almedina. 2006;

MARTINS, Lourenço – *Vide* MARQUES, Garcia;

MATOS, Filipe Albuquerque – *Responsabilidade Civil por Ofensa ao Crédito ou ao Bom Nome*. Coimbra. 2007. Tese de doutoramento;

MEORO, Mario E. Clemente; MÚGICA, Santiago Cavanillas, *Responsabilidad Civil y contratos en internet – su regulación en la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico*. Granada: Editorial Comares. 2003;

MONTEIRO, António Pinto – *Cláusulas limitativas e de exclusão da Responsabilidade Civil*. Coimbra: Almedina. 2003 (reimpr.);

- “A Responsabilidade Civil na negociação informática”. In *Direito da Sociedade da Informação*. Vol. I. Coimbra: Coimbra Editora. 1999;

MONTEIRO, Jorge Ferreira Sinde – *Responsabilidade por Conselhos, Recomendações ou Informações*. Coimbra: Almedina. 1989;

MÚGICA, Santiago Cavanillas, “Responsabilidad Civil”. In MÚGICA, Santiago Cavanillas (coord.), *Deberes y responsabilidades de los servidores de acceso y alojamiento: un análisis multidisciplinar*. Granada: Editorial Comares. 2005;

- Vide MEORO, Mario E. Clemente;

NETO, Luísa – *Novos Direitos: ou novo(s) objecto(s) para o Direito?*, Porto: U. Porto editorial. 2010;

OHM, Paul – “The rise and fall of invasive ISP surveillance”. In *Colorado Law*. Disponível em <http://ssrn.com/> (consult. em 27.07.2011);

PARENTI, Alberto - “L’armonizzazione comunitaria in materia di commercio elettronico”. In *Il Commercio elettronico. Profili giuridici e fiscali internazionali*. Egea. 2001;

PEIDRO, Lúcia Marín – *Los contenidos ilícitos y nocivos en Internet*. Madrid: Fundación Retevision. 2000;

PEREIRA, Alexandre Libório Dias – “Princípios do Comércio Electrónico”. In *Miscelâneas do Instituto de Direito das Empresas e do Trabalho*, n.º 3. Coimbra: Almedina. 2004;

- *Comércio electrónico na Sociedade da Informação: Da segurança técnica à confiança jurídica*, Coimbra: Almedina. 1999;

PEREIRA, Joel Timóteo Ramos – *Compêndio Jurídico da Sociedade da Informação*. Lisboa: Quid Juris. 2004;

- *Direito da Internet e Comércio Electrónico*. Lisboa: Quid Juris. 2001;

PINTO, Paulo Mota – “O direito à reserva sobre a intimidade da vida privada”. In *Boletim da Faculdade de Direito* [Separata]. Vol. LXIX. Coimbra. 1993;

POCH, Miguel Peguera – “La exención de responsabilidad civil por contenidos ajenos en Internet”. In *Revista Aranzadi de Derecho y Proceso Penal*. N.º 8. Navarra: Aranzadi – A Thomson Company. 2002;

PORTUGAL, Ministério da Justiça. Gabinete de Política Legislativa e Planeamento – *Lei do Comércio Electrónico anotada*. Coimbra: Coimbra Editora. 2005;

PROENÇA, José Carlos Brandão – *A conduta do lesado como pressuposto e critério de imputação do dano extracontratual*. Coimbra: Almedina. 1997;

REED, Chris - *Internet Law: Text and Materials*. 2ª ed. Cambridge: Cambridge University Press.2004;

RODRÍGUEZ, José Julio Fernández – “Seguridad y libertad: ¿equilibrio imposible? Un análisis ante la realidad de Internet”. In RODRÍGUEZ, José Julio Fernández; PASCUAL, Daniel Sansó-Rubert – *Internet: un nuevo horizonte para la seguridad y la defensa – II congreso sobre Seguridad, Defensa e Internet, Santiago de Compostela, noviembre de 2006*. Santiago de Compostela: Universidade de Santiago – Servizo de Publicacións e Intercambio Científico – Campus Universitario Sur. 2010;

ROLAND, Nicolas; VALGAEREN, Erik – “Youtube and social networking sites – new kids on the block?”. In STROWEL, Alain; TRIAILLE, Jean – Paul (coord.) – *Google et les nouveaux services en ligne: impact sur l'économie du contenu et questions de propriété intellectuelle*. Bruxelas: Lacier. 2008;

ROS, Rafael Mateu de - *Vide* GALLEGO, Mónica López-Morús;

SERRA, Adriano Paes da Silva Vaz – “Responsabilidade de pessoas obrigadas à vigilância”. In *Boletim do Ministério da Justiça*. Nº 85. Lisboa. 1959;

SMITH, Graham J. H. – *Internet Law and Regulation*. 2ª ed. Londres: Bird & Bird. 1997;

SOTTOMAYOR, Maria Clara – “Responsabilidade Civil dos pais pelos factos ilícitos praticados pelos filhos menores”. In *Boletim da Faculdade de Direito*. Vol. LXXI. Coimbra.1995;

SPLOIDORO, Marco - *Vide* MAGNI, Sabrina;

TRABUCO, Cláudia – “Conteúdos Ilícitos e Responsabilidade dos prestadores de serviços nas redes digitais”. In *Direito da Sociedade da Informação*. Vol. VII. Coimbra: Coimbra Editora.2008;

URÍBARRI, José Manuel Villar - *Vide* GALLEGO, Mónica López-Morús;

VALGAEREN, Erik - *Vide* ROLAND, Nicolas;

VARELA, João de Matos Antunes – *Das Obrigações em Geral*. Vol. I. 10º ed. Coimbra: Almedina. 2010 (reimpr.);

VAZ, Sónia Queiroz – “A nova legislação francesa sobre obrigações dos ISP’s quanto à retenção dos dados dos infractores e o respeito dos direitos de propriedade intelectual”. In *Lusíada. Direito*. Série II, n. 7. Lisboa: Editora Universidade Lusíada.2010;

VICENTE, Dário Moura – *Direito Internacional Privado: Problemática internacional da Sociedade da Informação*. Coimbra: Almedina. 2005.

- “Lei Aplicável à responsabilidade pela utilização ilícita de obras disponíveis em redes digitais”. In *Direito da Sociedade da Informação*. Vol. III. Coimbra: Coimbra Editora. 2002;

VIEIRA, José Alberto – “Download de obra protegida pelo Direito de Autor e uso privado”. In *Direito da Sociedade da Informação*. Vol. VIII. Coimbra: Coimbra Editora. 2009;

WONG, Cynthia - *Intermediary Liability: Protecting Internet platforms for expression and innovation*. Center for Democracy & Technology. 2010. Disponível em <http://www.cdt.org/> (consult. em 27.07.2011);

Relatórios, comunicados e artigos de imprensa (por ordem alfabética)

DEJAN, Sylvain; PÉNARD, Thierry; SUIRE, Raphael - Une première évaluation des effets de la loi HADOPI sur les pratiques des Internauts français. Disponível em <http://www.marsouin.org> (consult. em 27.07.2011);

ESTADOS UNIDOS DA AMÉRICA. Senado - Senate Judiciary Committee Report. N.º 105. Disponível em <http://www.congress.gov> (consult. em 27.07.2011);

REINO UNIDO. Câmara dos Lordes. Comissão de ciência e tecnologia. Primeiro relatório sobre a segurança pessoal na Internet (10.07.2007). Disponível em <http://www.publications.parliament.uk> (consult. em 27.07.2011).

ROLÓN, Fernanda Galdo – “Ley Sinde y la lucha contra la piratería”. In *Economia Ibérica* (01.04.2011);

UNIÃO EUROPEIA. Agência Europeia para a Segurança das Redes e Informação. Segurança, Economia e Mercado Interno, (31.01.2008), disponível em <http://www.enisa.europa.eu> (consult. em 27.07.2011);

UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. Comunicado de imprensa n.º 37/11 (14.04.2011). Disponível em <http://europa.eu> (consult. em 27.07.2011);

Lista de jurisprudência citada (por ordem cronológica)

Nacional

Acórdão do Tribunal da Relação de Coimbra de 03 de Junho de 2008 (Relator: BARATEIRO MARTINS). In Colectânea de Jurisprudência, 2008, III.

Acórdão do Supremo Tribunal de Justiça de 21 de Novembro de 2002 (Relator: FERREIRA GIRÃO). Disponível em <http://www.dgsi.pt> – Processo 02B2966 (consult. em 27.07.2011);

Acórdão do Supremo Tribunal de Justiça de 11 de Julho de 1978. In Boletim do Ministério da Justiça. N.º 279. Lisboa. 1978;

Acórdão do Supremo Tribunal de Justiça de 2 Março de 1978. In Boletim do Ministério da Justiça. N.º 275. Lisboa. 1978;

Acórdão do Supremo Tribunal de Justiça de 6 de Julho de 1971. In Boletim do Ministério da Justiça. N.º 209. Lisboa: 1971.

Do Tribunal de Justiça da União Europeia

Acórdão do Tribunal de Justiça das Comunidades Europeias. N.º C-275/06. In Jornal Oficial da União Europeia (8.03.2008). Europa. 2008.

Estrangeira

Décision n.º 2009-580 DC du Conseil Constitutionnel (2009). Disponível em www.conseil-constitutionnel.fr (consult. em 27.07.2011);

Tiffany(NJ) Inc v. Ebay (2008). Disponível em www.internetlibrary.com (consult. em 27.07.2011)

Louis Vuitton Moët Hennessy (LVMH) vs. Ebay (2008). Disponível em www.legalis.net (consult. em 27.07.2011);

Jean Yves L. dit Lafesse vs. Myspace (2007). Disponível em www.legalis.net (consult. em 27.07.2011);

Perfect 10, Inc. v. CCBill LLC (2007). Disponível em <http://caselaw.findlaw.com/> (consult. em 27.07.2011).

Sabam v. S.A. Tiscali (Scarlet) (2007). In MADY, BOURROUILLOU & HUGHES - CAELJ Translation Series #001. Cardoso Arts & Entertainment journal. N.º 25;

Corbis, Inc. v. Amazon.com (2004). Disponível em www.internetlibrary.com (consult. em 27.07.2011);

Proceso nº B-85235/02 del Tribunal da Cámara Civil y Comercial de la provincia de Jujuy, Argentina (2002). Apud JOEL TIMÓTEO RAMOS, Compêndio jurídico..., p. 876ss;

Yahoo! Inc. v. La Ligue Contre el Racisme el L'Antisemitisme (2001). Disponível em <http://caselaw.findlaw.com/> (consult. em 27.07.2011);

Estelle Haliday v. Altern Org. (1998). Disponível em www.legalis.net (consult. em 27.07.2011);

Godfrey v. Demon Internet (1998). Disponível em www.justice.gov.uk (consult. 27.07.2011);

Religious Technology Center v. Netcom Online Communications Services Inc. (1995). Disponível em www.loundy.com/CASES/ (consult. em 27.07.2011);

Playboy Enterprises Inc. v. Frena (1993). Disponível em www.loundy.com/CASES/ (consult. em 27.07.2011);

Cubby Inc. v. Compuserve Inc. (1991). Disponível em <http://www.loundy.com/CASES/> (consult. em 27.07.2011).

ÍNDICE

RESUMO	5
ABSTRACT	7
Agradecimentos.....	9
Sumário	11
Abreviaturas	13
 INTRODUÇÃO	 15
 CAPÍTULO I – A INTERNET E O DIREITO	 19
1. A Internet e os seus conteúdos	19
1.1. Ponto Prévio: da noção de conteúdo colocado e difundido na Internet.....	19
1.2. Da criação da Internet à <i>web 2.0</i>	19
1.3. Os conteúdos gerados por utilizadores	26
1.4. Balanço preliminar: a necessidade do Direito intervir no “mundo digital”	28
2. Os intervenientes na colocação e difusão de conteúdos na Internet	30
2.1. A dificuldade de criação de um critério estanque e uniforme para a sua concreta definição	30
2.2. Da delimitação em função do sujeito para a delimitação em função da actividade	31
2.3. Modelo seguido	32
 CAPÍTULO II – PONTOS CRÍTICOS NA DETERMINAÇÃO DA RESPONSABILIDADE CIVIL DO UTILIZADOR QUE COLOCA E DIFUNDE CONTEÚDOS ILÍCITOS NA INTERNET	 37
3. Ponto prévio: breve referência à dogmática comum da responsabilidade civil	37
3.1. A noção de responsabilidade civil	37
3.2. Pressupostos da responsabilidade civil.....	38
4. A ilicitude dos conteúdos colocados e difundidos na Internet	39
4.1. A dificuldade na determinação da ilicitude na Internet: breve alusão ao carácter transnacional da Internet.....	39
4.2. O conteúdo ilícito – Delimitação do conceito	43

4.3. As potenciais violações de bens jurídicos efectuadas por conteúdos colocados e difundidos na Internet.....	44
4.3.1. Violação de direitos de personalidade	44
a) O direito à honra e ao bom nome	44
b) O direito à reserva da intimidade da vida privada	45
c) O direito à imagem.....	45
4.3.2. Violação de direitos de propriedade intelectual.....	47
4.3.3. Violação de direitos de propriedade industrial	48
4.3.4. Violação do direito de propriedade <i>tout court</i>	49
5. A determinação da culpa do agente na colocação e difusão de conteúdos	50
5.1. O critério do <i>bonus pater familiae</i> na colocação e difusão de conteúdos <i>online</i>	50
5.2. Os actos ilícitos cometidos por inimputáveis. A reapreciação da <i>culpa in vigilando</i> ..	52
5.3. A Internet enquanto excludente da culpa do agente	56
6. O dano	57
6.1. A potenciação do dano na Internet	57
6.2. A reformulação de bens jurídicos alvo de protecção na Internet	59
7. O nexo de causalidade entre o dano e o facto ilícito: em especial, a potenciação do dano e a sua imputação ao(s) agente(s)	62
8. A exclusão da responsabilidade civil na Internet	64
8.1. A culpa do lesado	64
8.2. A autocolocação em perigo. O exemplo paradigmático das redes sociais	65
9. O problema do anonimato na Internet.....	66
9.1. O anonimato enquanto corolário do direito à reserva da intimidade da vida privada..	66
9.2. Formas de que se pode revestir o anonimato.....	68
9.3.Conclusão: a impraticabilidade da responsabilidade civil dos autores do acto ilícito...	69
 CAPÍTULO III – A RESPONSABILIDADE CIVIL DOS PRESTADORES DE SERVIÇOS INTERMEDIÁRIOS NA REDE.....	71
10. Evolução histórica da responsabilização dos prestadores de serviços intermediários	71
10.1. Estados Unidos da América.....	72
10.2. União Europeia	76
10.3. O panorama português.....	79
11. O panorama vigente: o Regime Jurídico do Comércio Electrónico.....	80

11.1. Âmbito de aplicação	80
11.2. Princípio da equiparação	81
11.3. Ausência de um dever geral de vigilância	81
11.4. A responsabilidade em caso de simples transporte ou fornecimento de acesso	83
11.5. A responsabilidade em caso de armazenagem	84
a) Armazenagem temporária.....	84
b) Armazenagem principal.....	85
11.6. A associação de conteúdos	87
11.7. A solução provisória de litígios	89
12. Enquadramento dogmático da responsabilidade civil dos intermediários	90
12.1. Enquadramento da responsabilidade civil dos intermediários como responsabilidade por acção ou omissão.....	90
12.2. Extensão dos deveres de agir que impendem sobre os intermediários?	92
12.3. A distribuição do ónus da prova	93
12.4. Conciliação da responsabilidade civil dos intermediários de armazenamento com a responsabilidade do utilizador que coloca o conteúdo ilícito <i>online</i>	94
13. Análise crítica da solução legal acolhida	95
13.1. A necessidade da precisão dogmática dos conceitos normativos do artigo 16.º RJCE.....	95
a) A problemática do conhecimento do conteúdo ilícito	95
b) A ilicitude manifesta.....	100
c) Determinação da diligência exigida quanto à retirada do conteúdo ilícito após a notificação da sua existência.....	101
13.2. Ausência de deveres de diligência para os serviços de mero transporte ou de acesso à rede	102
13.3. Ausência de normativização da “ausência de benefício económico directamente derivado da actividade ilícita.....	103
13.4. Potencial conflito entre a retirada dos conteúdos por parte dos intermediários e a liberdade de expressão e informação proporcionada pela Internet.....	104
14. Breves considerações sobre os contratos de prestação intermediária de serviços na Internet, em particular na <i>web 2.0</i> , e a sua aplicabilidade relativamente a conteúdos ilícitos colocados e difundidos em rede	106

14.1. A subscrição de serviços e a celebração do contrato na <i>web 2.0</i> , em particular as cláusulas de exclusão da responsabilidade	106
14.2. A emergência de deveres de protecção dos prestadores de serviços intermediários face aos consumidores com os quais celebram contratos.....	108
14.3. A emergência de deveres de protecção dos prestadores de serviços intermediários face a terceiros	111
14.4. Conclusão	113
15. Balanço do sistema acolhido: A primazia da eficiência do comércio electrónico sobre a tutela efectiva do lesado	113
CAPÍTULO IV – AS NOVAS TENDÊNCIAS FACE AO REGIME VIGENTE, NO ARQUÉTIPO DA <i>WEB 2.0</i>	
16. A exclusão do regime de isenção da responsabilidade com base na ausência da neutralidade típica da actividade de intermediação de serviços <i>online</i>	115
16.1. Termos em que se verifica. Alguns casos jurisprudenciais	115
16.2. Análise crítica	118
17. A obrigação de monitorização <i>a priori</i> de conteúdos. A colocação de filtros	120
17.1. Termos em que se verifica. O exemplo belga	120
17.2. Análise crítica	127
18. Reincidências sobre a responsabilidade do dono da coisa. O exemplo paradigmático da Lei HADOPI	129
18.1. Termos em que se verifica.....	129
18.2. Análise crítica	133
19. O Tratado ACTA.....	135
19.1. Termos em que se verifica.....	135
19.2. Análise crítica	136
20. Caminhos a trilhar?	138
CONCLUSÕES.....	
BIBLIOGRAFIA.....	
ÍNDICE	