João Pedro Sargaço Dias Raimundo

UMA NOVA FRENTE DA PROTEÇÃO DE DADOS PESSOAIS: A (IM)POSSIBILIDADE DE ASSEGURAR UM EVENTUAL DIREITO AO ESQUECIMENTO

Mestrado em Direito

Área de Ciências Jurídico-Políticas

Dissertação elaborada sob a orientação da

Professora Doutora Luísa Neto

Julho 2012

Índice

Resumo

Esta dissertação debruça-se sobre o direito ao esquecimento num contexto de emergência das novas tecnologias de informação, recentemente postulado na nova proposta da Comissão Europeia no âmbito da proteção de dados pessoais. Ao longo deste trabalho, iremos analisar o impacto desta reforma, ainda por implementar, que se debate com a delicada tarefa de equilibrar um reforço das garantias dos cidadãos com os interesses economicistas de um mercado digital onde os dados de natureza pessoal assumem um papel de moeda de troca com elevada "taxa de câmbio". Deste modo, e de forma tão aprofundada quanto possível, iremos, também, colocar em confronto o paradigma experienciado em torno das questões da privacidade em diferentes quadros legislativos, com destaque para a União Europeia e os Estados Unidos da América, ordenamentos com perspetivas tradicionalmente antagónicas nesta matéria.

Abstract

This dissertation focuses on the right to be forgotten in a context of emergence of new information technologies, recently proclaimed on the new European Comission's proposal regarding data protection. Throughout this paper, we will analyze the impact of this yet to be implemented framework, which struggles with the delicate task of balancing the enforcement of the citizens' rights with the economical interests of a digital market where personal data plays a role of a currency with a high "exchange rate". As such, and as thoroughly as possible, we will confront the paradigm experienced around the issues relating privacy in different legal frameworks, emphasizing the European Union and the United States of America, which have traditionally opposed legal systems concerning this subject.

Ao meu avô.

Agradecimentos

Ainda que este trabalho, que agora termino, seja - apenas por mim - assinado, tal não significa, de modo algum, que não deva um sentido reconhecimento a todos aqueles que, de forma direta ou indireta, deram o seu contributo para que esta dissertação chegasse a bom porto.

Assim, nesta oportunidade, gostaria de expressar a minha sentida gratidão:

À minha Orientadora de Mestrado, Professora Doutora Luísa Neto, com quem tive o enorme privilégio de poder trabalhar, mercê de toda a disponibilidade, conhecimento, paciência e profissionalismo que dedica a todos os projetos em que se envolve, sendo o apoio prestado nesta dissertação um ótimo exemplo;

Ao meu Ilustre Colega e Patrono, Dr. Victor Paulos, pela desmedida compreensão ao longo de todos estes meses em que, nem sempre, o meu trabalho no escritório pôde ser prioritário;

À minha família, especialmente aos meus pais e irmã, principais vítimas das minhas muitas oscilações de humor ao longo dos últimos meses, pelo apoio incondicional que me concederam em todas as fases da minha vida, por continuarem a ser a minha fonte de energia para ultrapassar os obstáculos e com quem faço questão de festejar todos os sucessos alcançados;

A todos os meus amigos, com especial menção ao Óscar, Tiago e, principalmente, à Solange, incansáveis a oferecer-me os seus préstimos quando a eles recorri, nem sempre com o melhor sentido de oportunidade, mas onde sempre encontrei uma resposta positiva;

À Melanie, quem mais de perto me acompanhou neste processo, a quem recorri nos momentos de desinspiração, e que bem sabe o papel que desempenha na minha vida. *We're in this together.*

Por último, deixo um profundo agradecimento a todos os colegas, docentes e funcionários, da Faculdade de Direito da Universidade do Porto, que preencheram o meu quotidiano académico nos últimos 6 anos, percurso que agora se dá por terminado e que certamente deixará saudades, na certeza, porém, de que os conhecimentos que adquiri nesta instituição não se quedarão pelos jurídicos e me acompanharão ao longo de toda a minha vida pessoal e profissional.

Lista de abreviaturas

Ac.	Acórdão
Cfr.	Conferir
Cit(s).	Citado(s)
Consult.	Consultado em
CNPD	Comissão Nacional de Proteção de Dados
CRP	Constituição da República Portuguesa
Ed.	Edição
EUA	Estados Unidos da América
FTC	*Federal Trade Commision*
loc.	local
n.$^{o(s)}$	número(s)
ob.	obra
p. (pp.)	página(s)
ss.	seguintes
UE	União Europeia
Vol.	Volume

INTRODUÇÃO

1. As preocupações com a privacidade não são assunto novo e têm vindo a sofrer profundas alterações ao longo dos tempos. Foi o advento do século XX que trouxe, efetivamente, as grandes mudanças, quer sociais, quer tecnológicas, que mais revolucionaram o modo como hoje encaramos o conceito de privacidade, favorecendo a disseminação de informação a um ritmo nunca visto, esta nem sempre disponibilizada com o assentimento do seu proprietário.

Na verdade, sempre que nos registamos numa rede social, fazemos compras numa *e-store* ou marcamos uma viagem de avião *online*, estamos a ceder informações pessoais, como o nosso nome, morada, número de telefone e número de cartão de crédito que, facilmente, poderão ser utilizadas de forma abusiva.

A expansão tecnológica propulsionada pelo dealbar da Internet, no início dos anos 90, mostrou-se decisiva para a construção desta janela orwelliana com vista privilegiada para a vida de cada um, como assinala, aliás, DAVID BRIN, na sua obra *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?*, onde, influenciado pela premissa *who watches the watchers?*, se mostra defensor da construção de uma sociedade translúcida, paradoxalmente, a única forma de os indivíduos, num plano de igualdade informativa, detetarem eventuais intromissões na sua privacidade[1].

Diariamente, 250 milhões de pessoas fazem uso da Internet, na Europa. O surgimento do comércio *online*, as redes sociais, as ligações à Internet de alta velocidade e sem fios, tudo isto contribuiu para uma alteração no paradigma de como interagir neste universo autossustentado pelos próprios utilizadores e que parece não ter limites para a quantidade de informação que pode albergar. Esta é a chamada *Web 3.0*, onde o conteúdo enviado pelos próprios internautas é combinado com técnicas avançadas de organização dos seus dados pessoais e preferências. Estes são relacionados com uma intuição capaz de competir com a do ser humano, recorrendo ao auxílio de motores de busca capazes de desenterrar a informação mais esquecida nesta rede inteligente, onde as políticas de privacidade pecam, muitas vezes, pela falta de transparência, em formulários de leitura difícil, e que contam com um certo *laissez-faire, laissez-passer* dos próprios utilizadores.

[1] Neste sentido, DAVID BRIN, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?*, Nova Iorque, Basic Books, 1999.

2. Se "a Internet não esquece"[2], o maior constrangimento residirá no facto de ela nos fornecer as ferramentas para encontrar qualquer tipo de informação, sobre qualquer cidadão, por mais anonimamente que este conduza a sua vida. É cada vez mais difícil apercebermo-nos de quando os nossos dados pessoais estão a ser recolhidos, já que esta recolha se faz, na grande maioria das vezes, e como é apanágio desta era digital, de forma automática, sendo estes mesmos dados usados pelas empresas que fornecem os mais variados serviços *online*, para nos brindar com conteúdos selecionados em função das nossas preferências. No mesmo sentido, também as próprias autoridades públicas de inúmeros ordenamentos jurídicos têm vindo a fazer uso crescente das informações pessoais dos cidadãos, sob o pretexto da luta contra o terrorismo e outros crimes de similar gravidade.

3. É certo que a proteção de dados já é matéria dotada de (des)adequado enquadramento legislativo e, em vários ordenamentos jurídicos, foram criadas leis com o objetivo de dificultar a recolha e processamento não autorizados de dados pessoais, bem como para evitar o denominado *forum shopping*, em que os potenciais prevaricadores se estabelecem no ordenamento jurídico mais favorável à prossecução das suas atividades. Contudo, dada a alucinante velocidade a que a Internet se continua a expandir, com todas as vantagens (de resto, inegáveis) e desvantagens que isso acarreta, urgirá, igualmente, atualizar e agilizar mecanismos, com o propósito de acompanhar este fenómeno e assegurar que os dados dos seus utilizadores estarão a salvo de usos indevidos.

Assim, de ambos os lados do Atlântico, responsáveis pelas autoridades reguladoras para a proteção de dados têm reunido esforços no sentido de monitorizar a atividade de gigantes como a *Google*[3] e o *Facebook*, à medida que tentam erguer nova legislação capaz de proteger os interesses dos cibernautas sem, no entanto, amordaçarem o crescimento da economia digital.

Atualmente, é prática comum abraçar as potencialidades da Internet com o intuito de nos autopromovermos e expressarmos as nossas opiniões livremente, através de ferramentas como *blogs* e colocação de vídeos *online*, com as famigeradas redes sociais à cabeça. Contudo, tal exposição não deverá ser lograda à custa da privacidade de cada utilizador (uma

[2] KENT LAWSON, *Do We Need a Right to Be Forgotten on the Internet?*, in Private Wifi, 19.09.2011. (Consult. 12.12.2011). Disponível em: http://www.privatewifi.com/do-we-need-a-right-to-be-forgotten-on-the-internet/.

[3] Há aqui que distinguir, primordialmente, a empresa *Google Inc.*, criadora de inúmeros serviços *online*, e o *Google Search*, o seu motor de busca, vulgarmente designado apenas como *Google*. Neste trabalho, para efeitos de uma melhor compreensão, referir-nos-emos ao motor de busca como *Google Search* e à empresa, simplesmente, como *Google*.

grande parte, menores de idade) e não são raros os casos de pessoas que, mais tarde, fazem de tudo para ver essa mesma informação, por si disponibilizada livremente, retirada[4].

4. É, precisamente, esta a intenção da Comissão Europeia que, dezassete anos depois da promulgação da Diretiva n.º 95/46/CE, procura colmatar as falhas deixadas por um diploma que já se mostra insuficiente para agir contra as novas formas de partilha de dados pessoais que entretanto floresceram e ocuparam uma parte generosa do espetro da utilização da Internet.

É sobre o pretenso direito ao esquecimento, perspetivado numa das propostas da Comissão Europeia, que se debruçará este trabalho. Em linhas gerais, o direito ao esquecimento visa preservar a privacidade dos cidadãos que, assim, se veriam escudados por um direito a ver os seus dados removidos da *web*, na ausência de razões legítimas para que eles lá permaneçam e pelas quais foram recolhidas. Este projeto, a ir avante, revolucionará o modo como navegamos na Internet, convidando a uma interação mais segura e menos receosa de futuras "caças às bruxas", sem, no entanto, se revelar como uma solução plenamente impermeável à utilização abusiva dos dados pessoais alheios.

Neste trabalho faz-se a apologia do esquecimento, do começar de novo, da possibilidade do ser humano se poder reinventar ou, pelo menos, de ter uma nova oportunidade. Os dados pessoais do indivíduo são propriedade do próprio, que deverá, salvo raras exceções, ter a última palavra sobre o seu destino.

O caráter de cada um não poderá, simplesmente, ser julgado com recurso ao seu perfil numa rede social, ou pelo que um motor de busca descobriu sobre ele há toda uma vida atrás, não devendo o ser humano ser reputado apenas em função do seu "arquivo digital", ao qual, muitas vezes, nem tem acesso.

Por tudo isto, urge criar uma estrutura não tanto legislativa, como eminentemente pedagógica, em que se volte a colocar nas mãos dos cidadãos, cibernautas ou não, o controlo sobre as informações sobre si publicadas, sem prejuízo de serem levadas a cabo campanhas de sensibilização para uma maior reflexão no instante de colocar informação sensível *online*.

[4] Recordemos, contudo, as palavras de JOSÉ DE OLIVEIRA ASCENSÃO, *Direito Civil: Teoria Geral, Vol. I: Introdução, as Pessoas, os Bens*, Coimbra, Coimbra Editora, 1997, p. 111: "Quem sobe para o palco, não pode estranhar a intensidade da luz dos holofotes".

I – A PROTEÇÃO DOS DADOS DE NATUREZA PESSOAL COMO SALVAGUARDA DA INTIMIDADE DO SEU TITULAR

1. OS DADOS PESSOAIS E OS DIREITOS CONEXOS

O fenómeno da recolha de dados pessoais não é algo de novo, mas tem vindo a tornar-se numa realidade cada vez mais frequente, invasiva e silenciosa, munindo-se do precioso auxílio das novas tecnologias, com destaque para o desenvolvimento da Internet.

De facto, as vantagens proporcionadas por estas novas tecnologias e pelo tratamento automatizado de dados pessoais levou-nos a abraçar um estilo de vida algo displicente em que vamos aos poucos abdicando do nosso direito a não ver a nossa vida exposta nos pixéis de um qualquer ecrã de computador.

Recentemente, a Comissão Europeia avançou dados de um estudo que mostra que 74% dos cidadãos europeus entendem que revelar os seus dados pessoais é, cada vez mais, uma atividade comum nos dias de hoje, sendo que 43% dos utilizadores frequentes da Internet receiam já ter disponibilizado demasiada informação pessoal *online*. Alarmante é, também, o facto de apenas um terço dos europeus estar a par da existência de autoridades nacionais responsáveis por zelar pela proteção dos dados pessoais dos seus cidadãos[5].

Mas, antes de nos debatermos com estas questões, cabe, aqui, primordialmente, estabelecer aquilo que entendemos por dados pessoais. Dados pessoais dizem respeito a qualquer informação que seja relativa a um indivíduo e o torne, assim, identificável[6/7]. Desta forma, teremos que incluir nesta categoria, analogamente, aqueles dados que possam vir a ser atribuídos a um determinado titular através do recurso a meios técnicos para esse efeito. Falamos das interações realizadas através da Internet, devendo considerar-se, igualmente, os dados do endereço IP do utilizador como dados pessoais[8], uma vez que podem ser identificáveis, recorrendo a meios tecnológicos à disposição de terceiros[9/10].

---

[5] Vejam-se os dados da COMISSÃO EUROPEIA, *Why Do We Need an EU Data Protection Reform?*, p. 1. (Consult. 25.05.2012). Disponível em: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf.

[6] Quando os dados forem meramente estatísticos e não permitam identificar a pessoa, estes não se tratam de dados pessoais, pois não permitem que se volte a saber a quem pertenciam, lembra CATARINA SARMENTO E CASTRO, *Direito da Informática, Privacidade e Dados Pessoais*, Coimbra, Almedina, 2005, p. 71.

[7] A alínea a) do artigo 3º da Lei n.º 67/98, de 26 de outubro, explana, também, o que se entende por pessoa identificável, ou seja, uma pessoa suscetível "de ser identificada directa ou indirectamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social".

[8] O endereço IP (ou *Internet Protocol*) é responsável pela identificação das máquinas, das redes e pelo encaminhamento das mensagens entre elas. Quando nos referimos ao IP que estamos a usar num determinado

Mas os dados pessoais podem assumir variadas formas, podendo reportar-se à vida pública, privada ou profissional do indivíduo, pelo que, mais habitualmente, estes dados poderão tomar a aparência de um nome, um endereço de correio eletrónico, informações bancárias e de saúde ou, até, de fotografias e outras publicações numa rede social[11/12].

A própria Lei n.º 67/98 de 26 de Outubro, comummente designada Lei da Proteção de Dados (doravante, Lei n.º 67/98), define, legalmente, na alínea a) do artigo 3º, os dados pessoais como sendo "qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável («titular dos dados»)"[13]. Por seu lado, a Diretiva n.º 95/46/CE dispõe, na alínea a) do artigo 2º, de forma bem mais sucinta e generalizante (algo ambígua, até), que os dados pessoais são "qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»)"[14].

Com a chegada da era da informática, em muito responsável pela sociedade em que coexistimos hoje, a facilidade de transmissão de dados através da *World Wide Web* resultou, inclusivamente, na concessão de dignidade constitucional à proteção de dados pessoais.

O artigo 35º da Constituição da República Portuguesa (doravante, CRP) confere aos cidadãos portugueses um manto de garantias ao seu dispor para que possam preservar a inviolabilidade da sua personalidade e do seu direito à reserva da intimidade da vida privada, também este com assento constitucional[15].

---

momento, quando conectados à Internet, estamos a falar dum endereço numérico que identifica de forma única esse computador na rede. Para maior desenvolvimento, AUTORIDADE NACIONAL DE COMUNICAÇÕES (ANACOM), *O que é o IP – Internet Protocol – IP?*, 07.02.2007, atualizado 14 dez. 2011. (Consult. 23.03.2012). Disponível em: http://www.anacom.pt/render.jsp?contentId=907480.

[9] Veja-se CATARINA SARMENTO E CASTRO, *Direito da Informática…,* ob. cit., p. 71.

[10] Para J. J. GOMES CANOTILHO e VITAL MOREIRA, o próprio enunciado "dados pessoais", no artigo 35º da CRP, revela, desde logo, uma estreita relação entre os direitos fundamentais do direito à dignidade da pessoa humana, do desenvolvimento da personalidade, da integridade pessoal e da autodeterminação informativa (que desenvolveremos *infra*), com o respetivo tratamento informática a que são sujeitos. Cfr. J. J. GOMES CANOTILHO, VITAL MOREIRA, *Constituição da República Portuguesa Anotada, Vol. I*, 4ª Edição, Coimbra, Coimbra Editora, 2007, p. 551.

[11] A este propósito, COMISSÃO EUROPEIA, *Why Do We Need an EU Data Protection Reform?*, ob. cit., p. 1.

[12] Também aqui podemos incluir outros dados de identificação como o número do cartão de contribuinte e da segurança social, uma chapa de matrícula ou, mesmo, uma impressão digital.

[13] J. J. GOMES CANOTILHO, VITAL MOREIRA, *Constituição da República Portuguesa Anotada*…, ob. cit., p. 553, acusam este artigo de ser pouco denso quando define dados pessoais como qualquer informação relativa a pessoa singular identificada ou identificável.

[14] Também o Tribunal de Justiça das Comunidades Europeias (atual Tribunal de Justiça da União Europeia, nome por que passou a ser designado com a entrada em vigor do Tratado de Lisboa) se pronunciou num acórdão de 6 de novembro de 2003, que o conceito de dados pessoais encerra "seguramente o nome de uma pessoa, a par do seu contacto telefónico ou de informações relativas às suas condições de trabalho ou aos seus passatempos".

[15] *Vide* o n.º 1 do artigo 26º da CRP.

Deste artigo 35º da CRP podemos, ainda, extrair uma subcategoria de dados pessoais: os dados pessoais sensíveis. Atente-se o n.º 3 do referido artigo: "[a] informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis".

Os dados sensíveis, cujo tratamento está também previsto no n.º 1 do artigo 7º da Lei n.º 67/98[16], bem como no n.º 1 do artigo 8º da Diretiva n.º 95/46/CE[17], merecem a nossa particular atenção, uma vez que, pela sua natureza, o seu tratamento poderá trazer um risco agravado para a privacidade do seu titular.

JOSÉ DE OLIVEIRA ASCENSÃO, no entanto, denuncia a inclusão do conceito legal de dados sensíveis, considerando o seu regime como "particularmente restritivo", contrariando a amplitude com que foram fixados os conceitos base na Lei n.º 67/98 e na Diretiva 95/46/CE. Este autor mostra-se, assim, um dos principais detratores da Lei n.º 67/98, que acusa de ser "generalizante" e de não atender, na realidade, aos problemas provocados pela intromissão da Internet no nosso quotidiano. O autor vai mais longe e expõe aquilo que lhe parece ser uma situação de lacuna da lei quanto à utilização de meios informáticos no tratamento de dados pessoais[18].

Por sua vez, CRISTINA QUEIROZ faz a distinção entre três tipos de dados pessoais. Em primeiro lugar, temos os "dados pessoais sensíveis", supramencionados, previstos no n.º 3 do artigo 35º da CRP, e que versam sobre convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica. Ora, este tipo particular de dados pessoais está protegido por uma proibição quanto ao seu tratamento sem o prévio consentimento do titular, excecionando-se esta situação no caso de haver "autorização prevista por lei" e sempre "com garantias de não discriminação"[19].

---

[16] Transcreve-se o n.º 1 do artigo 7º da Lei n.º 67/98: "É proibido o tratamento de dados pessoais referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica, bem como o tratamento de dados relativos à saúde e à vida sexual, incluindo os dados genéticos".

[17] Transcreve-se o n.º 1 do artigo 8º da Diretiva n.º 95/46/CE: "Os Estados-membros proibirão o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde ou à vida sexual".

[18] Neste sentido, JOSÉ DE OLIVEIRA ASCENSÃO, *Estudos sobre Direito da Internet e da Sociedade de Informação*, Coimbra, Almedina, 2001, pp. 211 e 212.

[19] *Vide* n.º 3 do artigo 35º da CRP.

Em segundo lugar, há que considerar a categoria dos "dados pessoais sensíveis não previstos no n.º 3 do artigo 35º da CRP". Para distinguir este tipo de dados pessoais, CRISTINA QUEIROZ recorre ao n.º 4 do artigo 7º e ao artigo 8º, ambos da Lei n.º 67/98, e, ainda, ao artigo 6º da Convenção para a Proteção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, do Conselho da Europa[20]. Desta forma, são também englobados como dados pessoais sensíveis os dados relativos a condenações penais e suspeitas de atividades ilícitas, bem como os dados relativos ao estado de saúde e vida sexual, incluindo os dados genéticos. CRISTINA QUEIROZ inclui, ainda, nesta categoria, os dados referentes à situação financeira e patrimonial.

Por último, temos os "dados pessoais não sensíveis" (ou "geralmente acessíveis"), para cuja recolha não está prevista nenhuma proibição legal, nem se exigindo o consentimento expresso do seu titular[21].

É, precisamente, na necessidade de consentimento[22], que se situa uma parte importante da problemática em torno dos dados pessoais, bem como na obrigatoriedade do cumprimento do princípio da finalidade, segundo o qual o fim específico da recolha, tratamento e utilização dos dados pessoais terá que estar *a priori* determinado, sendo que este consentimento terá sempre que ser renovado para efeitos de comunicação, interconexão ou difusão de dados de caráter pessoal, como veremos *infra*[23/24].

Existem ficheiros e bases de dados de titularidade pública e ficheiros e bases de dados de titularidade privada. Ora, não surpreende que, em ambos os casos, o regime aplicado difira. A constituição de bases de dados de titularidade pública encontra-se dependente de disposição legal. Por outro lado, à constituição de bases de dados, mas de titularidade privada, exige-se,

---

[20] Dispõe o artigo 6º da Convenção para a Proteção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, do Conselho da Europa: "[o]s dados de carácter pessoal que revelem a origem racial, as opiniões políticas, as convicções religiosas ou outras, bem como os dados de carácter pessoal relativos à saúde ou à vida sexual, só poderão ser objecto de tratamento automatizado desde que o direito interno preveja garantias adequadas. O mesmo vale para os dados de carácter pessoal relativos a condenações penais".

[21] A este respeito, CRISTINA QUEIROZ, *A Proteção Constitucional da Recolha e Tratamento de Dados Pessoais Automatizados*, in *Homenagem da Faculdade de Direito de Lisboa ao Professor Doutor Inocêncio Galvão Telles, 90 Anos*, Coimbra, Almedina, 2007, pp. 294 e 295.

[22] Dispõe a alínea h) do artigo 3º da Lei n.º 67/98: "«Consentimento do titular dos dados»: qualquer manifestação de vontade, livre, específica e informada, nos termos da qual o titular aceita que os seus dados sejam objecto de tratamento". A Diretiva n.º 95/46/CE ressalva, também, a importância do consentimento ao dispor, na alínea a) do artigo 7º, que "[o]s Estados-membros estabelecerão que o tratamento de dados pessoais só poderá ser efectuado se a pessoa em causa tiver dado de forma inequívoca o seu consentimento".

[23] Veja-se CRISTINA QUEIROZ, *A Proteção Constitucional…,* ob. cit., p. 295.

[24] É, ainda, de referir que os dados pessoais tornados "públicos" oficiosamente (ou seja, sem necessidade de consentimento expresso do próprio titular) não deixam de ser propriedade intelectual do sujeito titular dos mesmos. O cidadão não perde a titularidade dos seus elementos pessoais de identificação, mesmo quando estes figurem em documento público oficial. Neste sentido, CRISTINA QUEIROZ, *idem*, ob. cit., p. 296.

ainda, uma prévia notificação à autoridade nacional de controlo (em Portugal, a Comissão Nacional de Proteção de Dados)[25/26].

Da maior importância é, igualmente, assinalar os direitos de que está dotado o titular dos dados pessoais[27]. Assim, somos confrontados, desde logo, com o n.º 1 do artigo 35º da CRP, o qual confere aos cidadãos o "direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização", reconhecendo-lhes, ainda, "o direito de conhecer a finalidade a que se destinam, nos termos da lei".

Também os artigos 10º, 11º e 12º da Lei n.º 67/98 conferem estes direitos aos titulares dos dados, acrescentando, ainda, o direito de oposição (artigo 12º da Lei n.º 67/98, que transpôs o artigo 14º da Diretiva n.º 95/46/CE), permitindo que o titular se oponha, por "razões ponderosas e legítimas", a que as suas informações pessoais sejam objeto de tratamento.

Acrescente-se que todos estes direitos são irrenunciáveis, não podendo ser perspetivada qualquer via de limitação ou renúncia por parte dos titulares, inclusive através da realização de negócio jurídico[28]. O direito à proteção de dados pessoais, como direito fundamental[29], torna-se "virtualmente absoluto"[30], pelo que apenas exceções imperiosas poderão justificar tal derrogação que, todavia, terá que estar prevista na lei e apenas mediante um rigoroso controlo pelo princípio da necessidade, tendo em vista a segurança do Estado, a segurança pública, o combate a ilícitos criminais ou mesmo a própria proteção do titular dos dados (no caso de dados pessoais relacionados com a sua saúde)[31].

É à Comissão Nacional de Proteção de Dados (doravante, CNPD), entidade administrativa independente[32], com poderes de autoridade, que funciona junto da Assembleia da República[33], que a Lei n.º 67/98 atribui competência para exercer funções consultivas, de

[25] Tal, é-nos, inclusivamente, indicado pela própria Lei n.º 67/98, nos artigos 27º e seguintes.
[26] A este respeito, CRISTINA QUEIROZ, *A Proteção Constitucional…,* ob. cit., p. 301.
[27] Na verdade, já na Convenção para a Proteção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal (Convenção 108-1981), estavam previstos princípios fundamentais de proteção de dados, nomeadamente os princípios da finalidade, o princípio da qualidade (que pressupõe a adequação, pertinência, exatidão e atualização dos dados), ou garantias como a limitação do tratamento ao período de tempo estritamente necessário. Plasmados na Convenção estavam, ainda, o direito à informação e à retificação por parte do titular dos dados que lhe digam respeito. *Vide* artigo 5º, al. b) a e); artigo 8º, al. a) a d) da Convenção 108-1981.
[28] CRISTINA QUEIROZ, *A Proteção Constitucional…,* ob. cit., p. 304.
[29] *Vide*, novamente, o artigo 35º da CRP.
[30] MARIA EDUARDA GONÇALVES, *Direito da Informação: Novos Direitos e formas de Regulação na Sociedade de Informação*, Coimbra, Almedina, 2003, p. 94.
[31] Neste sentido, CRISTINA QUEIROZ, *A Proteção Constitucional…,* ob. cit., p. 305.
[32] De relembrar que a sua constituição está prevista no n.º 2 do artigo 35º da CRP.
[33] *Vide* artigo 2º da Lei n.º 43/2004, de 18 de agosto.

decisão administrativa, de investigação e, inclusivamente, funções sancionatórias em matéria de proteção de dados dos cidadãos, em todo o território nacional[34]. Mas a intervenção da CNPD estende-se além-fronteiras, cabendo-lhe, ainda, um importante papel de representação nacional junto da Comissão Europeia[35]. A Lei n.º 67/98 e a Diretiva n.º 95/46/CE, aliás, postularam "uma certa administrativização da matéria, com frequente subordinação a autorizações administrativas"[36].

Também a adoção, no plano das relações interprivados, do princípio da inversão do ónus da prova se mostra como mais uma arma ao dispor da proteção de dados pessoais na medida em que obriga a que seja o responsável pelo suposto tratamento abusivo a demonstrar que seguiu os procedimentos adequados a não causar caso dano ao seu titular[37].

De facto, a recolha e o tratamento de um conjunto ordenado de dados pessoais, pelo vasto valor informacional que confere ao responsável, sobre todo um universo de indivíduos, é uma tarefa que inspira particulares cuidados, pelo que se compreende que os responsáveis por este tratamento se encontrem sujeitos a inflexíveis obrigações, de cujo incumprimento decorrerão diversas sanções[38/39].

1.1. O DIREITO À AUTODETERMINAÇÃO INFORMATIVA

Reportando-nos, novamente, aos direitos dos titulares de dados pessoais, é ainda possível falar da existência de um direito geral à autodeterminação informativa, que vai de encontro ao postulado nos artigos 1º e 2º da CRP, que consagram, respetivamente, a dignidade da pessoa humana e o respeito e garantia de efetivação dos direitos e liberdades fundamentais[40].

---

[34] À CNPD, como autoridade responsável por zelar pelo cumprimento das disposições legais referentes à proteção de dados, bem como pelo efetivo cumprimento dos direitos legais dos cidadãos nesta matéria, é, ainda, atribuída uma função pedagógica e de esclarecimento.

[35] A este propósito, CATARINA SARMENTO E CASTRO, *Direito da Informática…,* ob. cit., p. 328.

[36] JOSÉ DE OLIVEIRA ASCENSÃO, *Estudos sobre Direito da Internet...*, ob. cit. p. 211.

[37] Neste sentido, CRISTINA QUEIROZ, *A Proteção Constitucional…,* ob. cit., p. 315.

[38] *Vide* CATARINA SARMENTO E CASTRO, *Direito da Informática…,* ob. cit., p. 65.

[39] Vejam-se os artigos 34º ss. da Lei n.º 67/98, artigo 193º do Código Penal e artigo 24º da Diretiva n.º 95/46/CE.

[40] Também no Brasil, a preocupação pela coleta e armazenamento de dados pessoais dos cidadãos foi, desde cedo, alvo de preocupação, pelo que, na Constituição Federal de 1988, foi criado o instituto do *habeas data*, uma das maiores inovações daquele diploma constitucional. O *habeas data*, expressão de origem latina que significa "apresentem-se os dados", trata-se de uma garantia constitucional que visa tutelar os direitos de personalidade - direito à imagem, direito à honra, direito à reserva da intimidade da vida privada - permitindo ao indivíduo aceder e retificar quaisquer informações existentes sobre si, em bancos de dados de entidades governamentais ou de caráter público. O *habeas data* exerce, assim, uma dupla função de prevenção e correção, conferindo ao cidadão o direito de solicitar, pela via judicial, que lhe seja facultada a exibição dos registos públicos ou privados que contenham informações a si respeitantes, para que delas se inteire e, se necessário, promova todas as

O direito à autodeterminação informativa é, como a própria expressão titula, um direito sobre a informação, que surge com o intuito de permitir ao indivíduo controlar aquilo que circula a seu respeito, impedindo que este se torne num "simples objeto de informações"[41], referindo-se, mais particularmente, aos dados armazenados através da utilização de meios informáticos. Este direito visa, assim, proteger e garantir um direito à intimidade privada no que concerne ao tratamento de dados pessoais[42], legitimado, mais uma vez, pelo frenético progresso tecnológico[43].

PAULO DA MOTA PINTO vai mais longe, entendendo que este direito à autodeterminação abrangerá, também, "a proteção perante a intrusão no domínio pessoal e a tutela perante a divulgação de afirmações pessoais e factos verdadeiros"[44]. Para este autor, o que aquele direito pretende é proteger o interesse em controlar o conhecimento e a difusão de informação relacionada com a vida privada do indivíduo, ou seja, sobre factos com ele intimamente relacionados, bem como com o seu meio, preservando o seu anonimato e, quando necessário, a sua salvaguarda do acesso físico de terceiros[45].

À luz do n.º 1 do artigo 18º da CRP, não nos podemos olvidar que as disposições constitucionais respeitantes à proteção de dados vinculam, também, as entidades privadas. "Todos estão sujeitos aos limites e obrigações enunciados neste artigo [artigo 35º da CRP] e

---

alterações que se relacionem com a imprecisão, desatualização ou inveracidade dos seus dados. A sua eficácia tem sido, contudo, posta em causa, por parte de alguma da doutrina. Alguns autores acreditam que o *habeas data* reflete em demasia a influência que recebeu do período pós-ditadura militar, ocorrida entre 1964 e 1985, encontrando-se, assim, desadequado aos dias de hoje. O advento da *World Wide Web* trouxe, também para os cidadãos brasileiros, preocupações no que tange a interconexão de dados e o uso desses mesmos dados para finalidades diversas. É aqui que o *habeas data* se mostra parco em eficácia, uma vez que, tal como está previsto no artigo 5º, parágrafo LXXII da Constituição Federal Brasileira e na Lei n.º 9507/97, de 12 de novembro de 1997, não consegue assegurar a tutela das informações que circulam na Internet, nomeadamente no que toca à recolha, uso e comercialização dos dados informatizados, por parte das empresas privadas. Não existindo qualquer regulamentação neste sentido, é possível prever que se verifiquem situações de abuso na utilização destes dados pessoais. Para um maior desenvolvimento a respeito desta matéria, MARCO AURÉLIO VENTURA PEIXOTO, *Habeas Data: A Polêmica Garantia Constitucional de Conhecimento e Retificação de Informações Pessoais em Poder do Estado*, in Jus Navigandi, Teresina, ano 6, n. 52, 01.11.2001. (consult. 10.01.2012). Disponível em: http://jus.com.br/revista/texto/2362; Ac. do STF, HD 75/DF, Rel. Min. Celso de Mello, DJU de 19.10.2006; FERNANDO JOAQUIM FERREIRA MAIA, *O Habeas Data Brasileiro na Perspetiva da sua Inefetividade e como Instrumento do Acesso à Justiça*. Disponível em: http://www.conpedi.org.br/manaus/arquivos/anais/recife/efetividade_fernando_joaquim_maia.pdf.

[41] J. J. GOMES CANOTILHO, VITAL MOREIRA, *Constituição da República Portuguesa Anotada*…, ob. cit., p. 551.

[42] A este respeito, CATARINA SARMENTO E CASTRO, *Direito da Informática…,* ob. cit., pp. 24 e 25.

[43] *Vide* CATARINA SARMENTO E CASTRO, *idem, ob. cit.*, p. 29. No mesmo sentido, HERMINIA CAMPUZANO TOMÉ, *Vida Privada y Datos Personales: Su Protección Jurídica Frente a la Sociedad de la Información,* Madrid, Editorial Tecnos, 2000, pp. 54 ss.

[44] PAULO DA MOTA PINTO, *A Limitação Voluntária do Direito à Reserva sobre a Intimidade da Vida Privada,* in *Estudos em Homenagem a Cunha Rodrigues, Vol. II*, Coimbra, Coimbra Editora, 2002, pp. 527 ss.

[45] PAULO DA MOTA PINTO, *idem*, ob. e loc. cits.

nas correspondentes leis concretizadoras"[46]. Assim, para que o direito à autodeterminação informativa seja dotado de eficácia, é necessário que o Estado assegure restrições à colheita, tratamento e utilização de dados de natureza pessoal, por parte destas entidades privadas, especialmente face aos riscos que a transmissão de dados e a Internet representam[47].

Particular relevância para este direito à autodeterminação informativa tem o direito dos indivíduos a conhecerem a finalidade dos dados recolhidos (princípio da finalidade, previsto no n.º 1 do artigo 35º, *in fine* da CRP). Os requisitos previstos no artigo 5º da Lei n.º 67/98 (correspondente ao artigo 6º da Diretiva nº 95/46/CE) permitem aos indivíduos o controlo dos fins para que são recolhidas as suas informações pessoais, evitando-se que o seu tratamento se processe tendo em vista finalidades não legítimas ou não especificadas, excessivas, ou que incluam dados desatualizados ou incorretos, bem como mantidos para além do tempo justificado[48].

O próprio Supremo Tribunal Administrativo veio confirmar, em Acórdão de 19 de junho de 1997[49], a correlação entre o direito à autodeterminação informativa e o direito à reserva da intimidade da vida privada, ao concluir, em sede de recurso contencioso, sobre uma decisão da então Comissão Nacional de Proteção de Dados Pessoais Informatizados (autoridade que precedeu a CNPD), que "as normas legais respeitantes à proteção de dados pessoais face à informática visam assegurar a reserva da vida privada e a garantia dos direitos do homem", pretendendo-se "salvaguardar um direito à privacidade"[50].

CATARINA SARMENTO E CASTRO complementa esta ideia, observando que este direito à autodeterminação informativa, hoje verdadeiro direito fundamental, permite ao indivíduo opor-se à recolha, tratamento e difusão dos seus dados pessoais contra o Estado e contra terceiros, não se restringindo a ser mero direito de defesa e de garantia do direito à reserva da intimidade da vida privada, mas sim, também, um "direito ofensivo" que permite decidir o que poderão os outros saber a nosso respeito[51]. Para esta autora, o direito à autodeterminação informativa é, assim, "um verdeiro feixe de prerrogativas que asseguram que cada um de nós

[46] J. J. GOMES CANOTILHO, VITAL MOREIRA, *Constituição da República Portuguesa Anotada*…, ob. cit., p. 556.
[47] Cfr. J. J. GOMES CANOTILHO, VITAL MOREIRA, *idem,* ob. cit., p. 554.
[48] Neste sentido, J. J. GOMES CANOTILHO, VITAL MOREIRA, *ibidem,* ob. cit., p. 553. Contudo, no contexto da Internet, onde os dados pessoais são recolhidos a um ritmo alucinante e usados para os mais variados fins, coloca-se em causa a efetivação deste princípio da finalidade. A este respeito, JEF AUSLOOS, *The 'Right to Be Forgotten' – Worth Remembering?,* in Computer Law and Security Review 2012, 09.12.2011, p. 13.
[49] Acórdão do Supremo Tribunal Administrativo de 19 de junho de 1997, Proc. n.º 042310, p. 27.
[50] *Idem.*
[51] Cfr. CATARINA SARMENTO E CASTRO, *Direito da Informática…,* ob. cit., p. 27.

não caminhe desprovido de um manto de penumbra, numa sociedade que deseja, cada vez mais, obrigar cada indivíduo a viver num mundo com paredes de vidro"[52].

1.2. A RESERVA DA INTIMIDADE DA VIDA PRIVADA E OS SEUS NOVOS DESAFIOS

O direito à autodeterminação informativa relaciona-se, como vimos, com o "direito ao livre desenvolvimento da personalidade" e o "direito à reserva da intimidade da vida privada e familiar", previstos no n.º 1 do artigo 26º da Lei Fundamental[53].

A reserva da intimidade da vida privada é, no fundo, o direito fundamental que aqui se visa preservar. Nas palavras de JOSÉ DE OLIVEIRA ASCENSÃO, "[a] proteção da vida privada tornou-se ponto alto do Direito de hoje"[54]. Este autor coloca a informática na tónica desta discussão, observando o facto de não haver limites para as suas capacidades, entendendo mesmo que a Lei n.º 67/98 tem, ou deveria ter, como objetivo, a proteção da vida privada e não a proteção de "meros dados pessoais identificáveis", objetivo esse que acaba por se esbater num "complexo de regras formais acumuladas"[55]. Neste sentido, ROLV RYSSDAL afirmou que "a finalidade real [das normas de proteção de dados] não é tanto a proteção de dados, mas sim a proteção das pessoas: mais precisamente, ainda, a proteção da vida privada das pessoas numa nova era que impõe a recolha e armazenamento de mais e mais dados sobre as suas vidas privadas e faz aumentar as possibilidades de manipulação e má utilização de tais dados"[56].

A importância deste direito à reserva da intimidade da vida privada está patente no facto de se tratar de um direito especial de personalidade e não de um direito geral de personalidade, como os plasmados nos artigos 70º e seguintes do Código Civil, e que encontra o seu reflexo no, já mencionado, n.º 1 do artigo 26º da CRP, que consagra o livre desenvolvimento da personalidade[57]. Também ORLANDO DE CARVALHO faz esta distinção, considerando o direito à reserva da intimidade da vida privada um "direito relativo à projeção

---

[52] CATARINA SARMENTO E CASTRO, *idem*, ob. e loc. cits.
[53] Note-se que o direito sobre a reserva da intimidade da vida privada está, também, consagrado no artigo 80º do nosso Código Civil, enquanto direito de personalidade.
[54] JOSÉ DE OLIVEIRA ASCENSÃO, *Estudos sobre Direito da Internet...*, ob. cit., p. 264.
[55] JOSÉ DE OLIVEIRA ASCENSÃO, *idem*, ob. cit., p. 211.
[56] ROLV RYSSDAL, *Proteção de dados e o Convénio Europeu dos Direitos Humanos*, Discurso de abertura da XIII Conferência de Comissários da Proteção de Datos, Novática, março, 1992, p. 9, *apud* HERMINIA CAMPUZANO TOMÉ, *Vida Privada…,* ob. cit., p. 56 (tradução nossa).
[57] A este respeito, CATARINA SARMENTO E CASTRO, *Direito da Informática…,* ob. cit., p. 22.

vital da personalidade"[58]. Aqui, o autor inclui o "direito ao caráter, o direito à história pessoal, o direito à verdade profunda e o direito à intimidade da vida privada"[59].

Na verdade, o reconhecimento do direito à reserva da intimidade da vida privada, e a sua consequente consagração na lei, é um fenómeno relativamente recente, alicerçado numa "sociedade transparente"[60] que expõe, irredutivelmente, as fragilidades do cidadão na preservação da sua vida privada.

SAMUEL WARREN e LOUIS BRANDEIS constituem duas personalidades incontornáveis no surgimento deste direito ao cunharem, num artigo escrito em 1890, a expressão *the right to be let alone*[61], pugnando, assim, por um "direito a ser deixado em paz" que possibilitaria impedir que determinadas informações referentes à vida privada dos indivíduos fossem recolhidas, estivesse ou não em causa a sua veracidade[62]. Estes dois autores abriram caminho para que a restante doutrina desenvolvesse a problemática, cujo estádio final resultou naquilo que hoje entendemos por direito à reserva da intimidade da vida privada.

Contributo generoso chega-nos, igualmente, por parte da jurisprudência alemã, com a criação da chamada "Teoria das Esferas de Proteção", oriunda de um Acórdão do Tribunal Constitucional Alemão, de 15 de dezembro de 1983[63]. O objetivo desta teoria era reconduzir cada nível de proteção a uma específica esfera de privacidade, organizada recorrendo a critérios pessoais e sociais de manifestação do indivíduo. Assim, para além de uma esfera de publicidade, poderíamos ainda admitir uma esfera pessoal, privada e íntima, cuja exposição teria, respetivamente, um maior impacto na violação da personalidade do indivíduo.

Seguindo, então, este critério de valoração, reconduzimos à esfera de publicidade todos os atos praticados em público pelo cidadão, cumulados com o desejo de que estes sejam efetivamente do conhecimento geral. Na esfera pessoal incluímos os atos praticados pelo indivíduo no seu ambiente social, sem que, no entanto, haja vontade na sua publicitação. Na esfera privada englobamos, já, as relações do indivíduo para com um número mais restrito de pessoas com quem tem uma maior proximidade emocional. Por último, assumimos a esfera

---

[58] ORLANDO DE CARVALHO, *Direitos de Personalidade* (apontamentos de aulas), Polic., Coimbra, p. 4 ss, *apud* CATARINA SARMENTO E CASTRO, *Direito da Informática…,* ob. cit., p. 23.
[59] CATARINA SARMENTO E CASTRO, *idem*, ob. e loc cits.
[60] Expressão cunhada por DAVID BRIN em *The Transparent Society: Will Technology Force Us to Choose Between Freedom and Privacy?*, New York, Basic Books, 1999.
[61] Para um maior desenvolvimento, SAMUEL WARREN, LOUIS BRANDEIS, *The Right to Privacy*, in Harvard Law Review, V. IV, n.º. 5, 1890, pp. 193 ss.
[62] Cfr. DOMINGOS SOARES FARINHO, *Intimidade da Vida Privada e Media no Ciberespaço*, Coimbra, Almedina, 2007, p. 44.
[63] Veja-se DOMINGOS SOARES FARINHO, *idem*, ob. cit., p. 44, nota 49.

íntima como sendo a mais sensível, envolvendo sentimentos intrínsecos à identidade do indivíduo e que apenas a ele dizem respeito[64/65].

Esta teoria afigura-se, na realidade, de uma utilidade extrema no sentido de delimitar o objeto a que se reporta o direito à reserva da intimidade da vida privada, para que se possa aferir qual a "vida privada" merecedora da proteção prevista tanto no n.º 1 do artigo 26º, como no n.º 3 do artigo 35º, ambos da CRP[66].

Constituindo o uso da Internet, muitas vezes, uma atividade intimista, em que o utilizador se sente refugiado atrás dum monitor, parece-nos, aqui, que também os seus dados pertencem àquilo que temos vindo a considerar como dados pessoais merecedores de integrar a reserva da intimidade da vida privada dos seus titulares.

MARIA EDUARDA GONÇALVES não deixa, contudo, de observar uma certa controvérsia em torno desta questão. A autora realça que, apesar da matéria de proteção de dados pessoais automatizados estar associada à reserva da intimidade da vida privada protegida pela CRP e por diplomas de cariz internacional[67], "os dados pessoais informatizados constituem informação que é, por natureza e por definição, suscetível de ser conhecida"[68]. Como tal, entende a autora que o que justifica a proteção destes dados é, precisamente, o facto destas informações serem utilizadas, através da informática, para os mais variados fins, fins esses tidos como legítimos. Seguindo este raciocínio, perde o sentido remeter estas informações para o seio da reserva à intimidade da vida privada, uma vez que esses dados são utilizados comummente tanto por entidades públicas, como por entidades privadas, na prossecução das suas atividades[69].

Esta autora salvaguarda, todavia, o risco destes dados poderem ser utilizados de forma abusiva para fins diversos daquilo para que foram recolhidos, pelo que, para ela, o interesse

---

[64] A este respeito, DOMINGOS SOARES FARINHO, *ibidem*, ob. cit., p. 45.

[65] Também ORLANDO DE CARVALHO - *Direitos de Personalidade…,* ob. cit., pp. 7 e 8, *apud* CATARINA SARMENTO E CASTRO, *Direito da Informática…,* ob. cit., pp. 23 e 24 - distinguiu, para este efeito, uma esfera privada, uma esfera pessoal e uma esfera de segredo. A primeira diria respeito a aspetos não públicos mas que poderiam não ser pessoais (como fotografias de animais domésticos). A segunda já seria mais restrita e implicaria os gostos pessoais e preferências do indivíduo, impondo-se, inclusivamente, ao próprio cônjuge. Por último, na esfera de segredo, caberiam coisas secretas como *passwords*, entradas num diário, historial médico, etc.

[66] *Vide* DOMINGOS SOARES FARINHO, *Intimidade da Vida Privada…,* ob. cit., p. 45.

[67] Veja-se o artigo 1º da Convenção para a Proteção das Pessoas relativamente ao Tratamento Informatizado de Dados Pessoais, do Conselho da Europa.

[68] MARIA EDUARDA GONÇALVES, *Direito da Informação…,* ob. cit., p. 85.

[69] Cfr. MARIA EDUARDA GONÇALVES, *idem*, ob. cit., pp. 85 e 86.

individual merecedor de proteção é o "interesse numa utilização condicionada dos dados" e não uma proibição da recolha e utilização dos dados pessoais de tratamento informatizado[70].

Destarte, estes regimes de proteção de dados procuram, a todo o momento, uma ponderação entre dois princípios: a garantia das liberdades e direitos individuais de cada cidadão e a liberdade de utilização e circulação da informação pessoal[71/72], sendo certo que "a salvaguarda da própria vida privada encontra-se no comportamento e controlo que o utilizador efetua e, na Internet, passa necessariamente pelo direito de realizar opções informadas, de forma que, sempre que se recolhem dados para o setor privado, o interessado possa escolher quais os dados que quer comunicar e para que finalidades"[73].

2. A INTERNET COMO VEÍCULO DISSEMINADOR DOS DADOS PESSOAIS

Ao longo do último subcapítulo, fomos dando algum destaque à influência da Internet no tratamento de dados pessoais.

De facto, no mundo de hoje, ininterruptamente ligado por uma Internet que não esquece, amplia-se o espetro de preocupação e desconforto, motivado pelas influentes redes sociais, por motores de busca capazes de ir buscar a informação mais recôndita e por uma imprensa digital atualizada ao minuto. O fim do período analógico, substituído por uma digitalização sem precedentes, trouxe consigo relevantes mudanças no modo como criamos e transmitimos informação, que é agora transformada em *bits*, e pode ser enviada para qualquer pessoa, em qualquer canto do mundo, pelos túneis da Internet, sem perder a sua qualidade e a custos tremendamente reduzidos[74/75].

---

[70] Note-se que esta proibição poderá, contudo, ser derrogada pela própria CNPD, que assim poderá conceder autorização prévia no exercício das suas capacidades previstas no artigo 28º da Lei n.º 67/98.

[71] No mesmo sentido, HERMINIA CAMPUZANO TOMÉ, *Vida Privada y Datos Personales*…, ob. cit., p. 70, entende que, quanto a esta problemática, o que está em causa é considerar primordial a segurança da vida privada que, assim, deverá prevalecer sobre qualquer situação, cabendo aos operadores de Direito chegar a um compromisso entre todos os interesses em jogo, aproveitando ao máximo as potencialidades que a tecnologia nos proporciona.

[72] *Vide* MARIA EDUARDA GONÇALVES, *Direito da Informação…,* ob. cit., p. 95.

[73] GARCIA MARQUES, LOURENÇO MARTINS, *Direito da Informática*, Coimbra, Almedina, 2006, p. 432.

[74] *Vide* GRAHAM J. H. SMITH *et al.*, *Internet Law and Regulation*, 2ª Ed., Londres, FT Law and Tax, 1997, p. 14.

[75] A CRP consagra, aliás, no n.º 4, do artigo 35º, a garantia de acesso às redes informáticas de uso público. J. J. GOMES CANOTILHO e VITAL MOREIRA, consideram esta garantia "uma nova dimensão da liberdade de expressão", sendo o acesso à rede uma condição prévia da própria liberdade de expressão através da Internet. Cfr. J. J. GOMES CANOTILHO, VITAL MOREIRA, *Constituição da República Portuguesa Anotada*…, ob. cit., p. 556.

A Internet, ou o ciberespaço[76], como também é conhecida, pode ser vista, mais objetivamente, como um conjunto de computadores ligados entre si. A sua chegada quebrou a barreira das capacidades humanas, constituindo-se num poderoso veículo de comunicação capaz de relacionar a transmissão de texto, de som, de imagem, em variados suportes, de forma autossustentada pelos próprios utilizadores, criando, assim, um "verdadeiro ecossistema virtual"[77].

Falamos da globalização e do avanço tecnológico como consequência lógica de quase todas as mudanças que têm acompanhado a evolução da sociedade e, como tal, o modo como os dados pessoais são recolhidos, tratados e difundidos foi, também, francamente influenciado[78/79]. Desde logo, assinala-se o aumento sem precedentes dos fluxos de dados, que faz com que a informação pessoal seja recolhida e trocada em quantidades extraordinárias por todo o mundo[80]. Estas questões apresentam-se como novos desafios às autoridades de proteção de dados pessoais, uma vez que não há fronteiras nem barreiras jurisdicionais que impeçam a entrada e saída de informação de país para país[81].

De facto, e uma vez abrindo mão da sua informação *online*, torna-se muito complicado, para o utilizador, conter e limitar até onde poderá ela ser distribuída. Na verdade, a esmagadora maioria da informação disponível na Internet encontra-se à disposição de qualquer utilizador que dela se pode apoderar sem que os seus titulares disso sejam informados.

---

[76] A génese desta expressão data de 1986, quando William Gibson a criou a partir de uma combinação da palavra grega *cyber* (controlo) e da palavra inglesa *space* (espaço). *Vide* DOMINGOS SOARES FARINHO, *Intimidade da Vida Privada…,* ob. cit., p. 13.

[77] DOMINGOS SOARES FARINHO, *idem*, ob. cit., p. 14. No mesmo sentido, DANIEL J. SOLOVE, *The Future of Reputation: Gossip, Rumor and Privacy on the Internet,* New Haven e Londres, Yale University Press, 2007, pp. 4 e 5.

[78] O Tribunal das Comunidades Europeias (antigo Tribunal de Justiça da União Europeia), em interpretação da Diretiva 95/46/CE, no Acórdão de 6 de novembro de 2003, já mencionado, considerou que, se alguém fizer referência, numa página de Internet, à identificação de alguém pelo seu nome ou por outros meios, tal constitui uma forma de tratamento de dados pessoais na aceção do artigo 3º, n.º1 da Diretiva. O entendimento da CNPD vai no mesmo sentido. Cfr. CATARINA SARMENTO E CASTRO, *Direito da Informática…,* ob. cit., p. 22.

[79] "A rápida introdução das tecnologias de informação e das comunicações e as aplicações correspondentes estão a acarretar mudanças profundas nas nossas sociedades, economias e sistemas jurídicos com consequências no modo como vivemos, aprendemos, interagimos socialmente, conduzimos negócios e nos governamos." K. W. GREWLICH, *Governance in Cyberspace. Access and Public Interest in Global Communications,* Kluwer Law International, Haia, 1999, p. xiii, *apud* MARIA EDUARDA GONÇALVES, *Direito da Informação…,* ob. cit., p. 138.

[80] Destaca-se aqui a importância do chamado sistema de *cloud computing,* que permite aos utilizadores alojar informação em servidores *online* e poder aceder-lhe remotamente, em qualquer lugar do mundo, sem necessidade de a ter consigo fisicamente.

[81] Cfr. COMISSÃO EUROPEIA, *How Will the EU's Reform Adapt Data Protection Rules to New Technological Developments?,* p. 1. (Consult. 25.11.11). Disponível em: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/8_en.pdf.

São vários os tipos de intervenientes a integrar este *habitat* virtual, o que aumenta em muito a possibilidade de as regras de proteção de dados pessoais virem a ser ou não respeitadas, destacando-se os operadores de telecomunicações, os fornecedores de acesso à Internet, os fornecedores de bens e serviços *online* e, claro, os utilizadores, ou cibernautas[82].

Com a multiplicação dos processos informáticos, é possível traçar o perfil de cada internauta, uma vez que a sua atividade na rede deixa um rasto de "pegadas eletrónicas" que permite identificar, com elevada acuidade, os sítios que visitou, por que palavras-chave orientou as suas pesquisas e que compras fez *online*, resultando numa autêntica "radiografia" da sua vida. Para cúmulo, toda esta informação é, agora, orientada de acordo com as próprias preferências do utilizador, previamente recolhidas, de modo a que a resposta dada pelos motores de busca já venha adequada a satisfazer aquelas que aparentam ser as necessidades do utilizador. Deparamo-nos, assim, com uma mudança de paradigma em que é a própria máquina a ter o papel ativo e a conduzir o utilizador àquilo que ele deseja ver[83/84].

Irónico, no meio de tudo isto, é pensar que este sistema de rastreamento é realizado, muitas vezes, com a conivência do próprio utilizador, que ao aceder à Internet, "autoriza" (ainda que sem qualquer intervenção sua) que pequenos ficheiros destinados a facilitar utilizações futuras se alojem no seu próprio terminal e lhe monitorizem os movimentos. Estes ficheiros denominam-se *cookies*[85].

A problemática do direito ao esquecimento, que está no cerne desta dissertação, é, também, francamente inflacionada quando o meio de comunicação usado para difundir a informação em causa é a Internet, onde vicissitudes, como a descartabilidade de um papel de jornal, ou a efemeridade de um programa de televisão já transmitido há algum tempo, não se

---

[82] A este respeito, CATARINA SARMENTO E CASTRO, *Direito da Informática…,* ob. cit., p. 154; veja-se, também, para maior desenvolvimento, JOÃO FACHANA, *A Responsabilidade Civil pelos Conteúdos Ilícitos Colocados e Difundidos na Internet,* Dissertação de Mestrado em Direito (Área de Especialização em Ciências Jurídico Privatísticas), Porto, Faculdade de Direito da Universidade do Porto, julho 2011, pp. 30 ss.

[83] Neste sentido, JOSÉ DE OLIVEIRA ASCENSÃO, *Estudos sobre Direito da Internet...,* ob. cit., p. 186.

[84] Este novo paradigma ficou conhecido por *Web 3.0*.

[85] Salvaguarda-se, também, os casos de todos os outros utilizadores, porventura, a grande maioria que desconhecerá o funcionamento dos ficheiros *cookies.* Os *cookies* consistem, assim, em ficheiros que denunciam a identidade do terminal do utilizador, pelo que, quando o utilizador acede a um determinado *website*, o servidor onde este está alojado envia para o computador do utilizador um *cookie*, que passará a identificá-lo sempre que este aceda de novo ao website. A partir daqui, é possível ao servidor (e, consequentemente, aos responsáveis pelo *website*) saber com que frequência o internauta se liga ao *website* e quais as suas preferências dentro deste. A este respeito, DOMINGOS SOARES FARINHO, *Intimidade da Vida Privada…,* ob. cit., pp. 68 e 69. A CNIL (*Commission Nationale de l'Informatique et des Libertés*), autoridade francesa para a proteção de dados, já se mostrou contra a utilização deste mecanismo por parte dos gestores de *websites*, em virtude de ser usado, na maioria das vezes, para monitorizar os utilizadores sem que disso se apercebam, com a desculpa de facilitar a sua navegação. Cfr. GARCIA MARQUES, LOURENÇO MARTINS, *Direito da Informática…,* ob. cit., p. 440.

verificam, expondo intemporalmente a vida privada dos indivíduos que se vêem incapazes de fugir ao passado, reféns de uma autêntica "letra escarlate digital"[86].

Noutro plano, temos, igualmente, a delicada questão do anonimato no ciberespaço. O conforto de uma máscara de ocultação da identidade torna-se extremamente apelativo e, de certa forma, instiga a que os utilizadores tenham a tentação de aceder à vida privada alheia, agravando o risco de condutas que atentem contra os direitos de personalidade das suas vítimas. Apesar de se poder argumentar que este anonimato pode, no entanto, trazer algumas vantagens no sentido de promover uma liberdade de expressão *online*, a ameaça de um voyeurismo descontrolado e uma navegação na Internet sem responsabilidades acrescidas será sempre um foco de tensão para a vida privada de terceiros, bem como um porto seguro para aqueles que se dedicam ao crime informático e saem impunes pela ausência de meios para descobrir a sua identidade[87].

Toda esta factualidade leva-nos a constatar que os mesmos problemas com que se confronta diariamente o indivíduo na sua rotina, no que tange à recolha, troca e difusão de informação pessoal, verificam-se - na realidade, intensificam-se - no ciberespaço, mostrando-se premente a necessidade de reforçar a proteção sobre os dados pessoais, no sentido de combater todas estas formas de intromissão que ameaçam a privacidade do internauta.

JOSÉ DE OLIVEIRA ASCENSÃO vaticina mesmo que "[t]alvez estejamos a assistir a uma nova formação de classes: a classe superior que domina porque tem a informação e a inferior, a quem é vedado o acesso a esta informação"[88], pelo que urge que estas considerações sobre proteção de dados sejam tomadas em conta pelos utilizadores da Internet, no momento de fornecerem informações pessoais a qualquer *website* ou base de dados *online*[89/90].

2.1. O IMPORTANTE PAPEL DO DIREITO NUM CIBERESPAÇO AINDA "REBELDE"

A tudo isto a que aludimos, não é alheio o Direito. A *World Wide Web*, embora não sendo uma área inteiramente regulada, é já um espaço onde existem normas que devem ser

[86] Veja-se DANIEL J. SOLOVE, *The Future of Reputation…,* ob. cit., pp. 76 ss.
[87] *Vide* GARCIA MARQUES, LOURENÇO MARTINS, *Direito da Informática…,* ob. cit., pp. 424 e 425.
[88] JOSÉ DE OLIVEIRA ASCENSÃO, *Estudos sobre Direito da Internet...,* p. 187. No mesmo sentido, JEF AUSLOOS, *The 'Right to Be Forgotten'…,* ob. cit., p. 10.
[89] Cfr. GRAHAM J. H. SMITH *et al.*, *Internet Law and Regulation*, ob. cit., p. 14.
[90] Recentemente, têm sido levadas a cabo algumas campanhas de sensibilização à publicação de dados pessoais, nomeadamente, em *websites* anfitriões de redes sociais, não apenas por parte de utilizadores anónimos conscientes para estes perigos, mas também por parte da própria Comissão Europeia. Para mais desenvolvimento, COMISSÃO EUROPEIA, *Think Before You Post!*, 09.02.10. (Consult. 05.04.12). Disponível em: http://ec.europa.eu/news/science/100209_1_en.htm.

respeitadas sob pena de sanções[91]. Não nos podemos esquecer que a Internet é um vastíssimo universo, onde não existem fronteiras geográficas e que qualquer ação legal deverá passar por um esforço de concertação máxima dos vários ordenamentos jurídicos envolvidos, tendo sempre presente as particularidades daquele mundo virtual[92]. Sendo certo que o Direito relacionado com a proteção de dados pessoais afirmou-se como um "fenómeno predominantemente europeu"[93], destaca-se, necessariamente, a importância do Direito Internacional nesta matéria, uma vez que o fornecedor de conteúdos pode estar sediado num país, alojar a informação num servidor que se encontre num país diferente e, ainda, provocar o dano em qualquer outro quadrante do planeta[94].

Como temos vindo a observar, a publicação de informação na Internet tem uma difusão e uma consequente capacidade de dano apenas comparável à dos grandes meios de comunicação social, como sejam as maiores cadeias televisivas ou os jornais com maior tiragem mundial, que, por sua vez, também já fazem da Internet uma perfeita plataforma de divulgação dos seus conteúdos. Na teoria, colocada uma informação na Internet, os seus destinatários são os milhões de computadores com acesso à *web*, cabendo ao utilizador ir ao encontro dessa mesma informação. Assim se justifica o entendimento de que, quando veiculadas pela Internet, as informações relativas à vida privada dos indivíduos são alvo de especial preocupação, na medida em que, não só se verifica uma avultada exposição da intimidade dos sujeitos em causa, como esta se torna irremediavelmente mais acessível a um maior número de destinatários[95].

MARIA EDUARDA GONÇALVES chama a atenção para o facto de aqui se confrontarem dois interesses: o do próprio indivíduo que pretende ver as informações sobre si salvaguardadas e o interesse das entidades públicas ou privadas que pretendem prosseguir a sua atividade com a eficiência que apenas as novas tecnologias lhes conseguem proporcionar[96].

---

[91] JOEL TIMÓTEO RAMOS PEREIRA, *Direito da Internet e Comércio Electrónico*, Lisboa, Quid Juris Sociedade Editora, 2001, afirma, no entanto, que "[a] Internet ultrapassou todas as barreiras económicas, sociais, étnicas, raciais e religiosas. Regular juridicamente tais matérias é pretender controlar o incontrolável."

[92] Cfr. DOMINGOS SOARES FARINHO, *Intimidade da Vida Privada…,* ob. cit., p. 17.

[93] IAN WALDEN, *Data Protection in Computer Law*, in CHRIS REED, JOHN ANGEL, *Computer Law*, 4ª Ed., Londres, Blackstone Press Limited, 2000, p. 442.

[94] Veja-se DOMINGOS SOARES FARINHO, *Intimidade da Vida Privada…,* ob. cit., p. 73.

[95] Nas palavras de DOMINGOS SOARES FARINHO, *idem,* ob. cit., p. 71, "[o] potencial de lesão do ciberespaço é o mais elevado possível de entre todos os cenários, quer pelo número de destinatários a que pode chegar quer pela dificuldade em localizar a fonte do dano. Tal deve ser considerado na análise do conflito de direitos".

[96] Cfr. MARIA EDUARDA GONÇALVES, *Direito da Informação…,* ob. cit., p. 82.

As próprias legislações nacionais e internacionais desde sempre tentaram adaptar-se e acompanhar esta evolução, tendo algumas não conseguido resistir à erosão do tempo e sido, consequentemente, reformadas. Há, contudo, quem ainda defenda que a Internet deveria manter-se uma zona neutra, imune a qualquer tipo de regulação que não seja a gerada dentro do próprio ciberespaço[97].

Esta posição de autorregulação, particularmente relevante nos Estados Unidos[98], tem-se apoiado, sobretudo, em argumentos pragmáticos para justificar o seu pensamento, na medida em que defende que a dimensão global da Internet impossibilita o estabelecimento de meios eficazes de controlo e regulação, frustrando-se quaisquer tentativas por partes das autoridades de regular o ciberespaço, com os indivíduos e organizações a esconderem-se por trás do anonimato que este mundo virtual lhes proporciona[99]. Os apologistas desta autorregulação encontram, contudo, diferentes motivações para a sua efetivação, pelo que, para uns, na sua origem estarão preocupações relacionadas com a limitação da liberdade de comunicação, enquanto que, outros, darão primazia ao aspeto económico, preferindo, simplesmente, remeter a sua regulação para o próprio mercado[100].

Esta autorregulação pressupõe um maior envolvimento por parte das empresas que tratam dados pessoais dos utilizadores na Internet, através de políticas de privacidade exigentes e responsáveis que assegurem um tratamento leal e congruente com os fins para que os seus dados são recolhidos, protegendo-os, inclusivamente, de qualquer intrusão por parte de terceiros[101].

GARCIA MARQUES e LOURENÇO MARTINS concluem, contudo, que "[a]pesar da importância da autorregulação na Internet, o certo é que não dispõe de valor injuntivo e juridicamente vinculante, a não ser na medida em que a mesma possa ser uma forma de geração do costume"[102].

Não obstante, não parece que alguém seja capaz de duvidar que a Internet, tal como qualquer outro meio de comunicação, deve obediência aos princípios fundamentais da

---

[97] *Vide* MARIA EDUARDA GONÇALVES, *idem,* ob. cit., p. 138.
[98] Cfr. GARCIA MARQUES, LOURENÇO MARTINS, *Direito da Informática…,* ob. cit., p. 425.
[99] A este propósito, MARIA EDUARDA GONÇALVES, *Direito da Informação…,* ob. cit., p. 138.
[100] Veja-se MARIA EDUARDA GONÇALVES, *idem,* ob. cit., p. 141.
[101] *Vide* GARCIA MARQUES, LOURENÇO MARTINS, *Direito da Informática…,* ob. cit., pp. 428 e 429.
[102] A este respeito, GARCIA MARQUES, LOURENÇO MARTINS, *Direito da Informática…,* ob. cit., p. 429. No mesmo sentido, mas com uma posição mais vincada, JEF AUSLOOS, *The 'Right to Be Forgotten'…,* ob. cit., p. 11, afirma: *… it has become clear over the last few years that it is impossible to rely on the market alone to give (back) control to individuals. Code and especially the law will be necessary to assure a healthy and balanced market.*

liberdade de expressão e de informação, pelo que a própria apologia de uma liberdade de acesso e utilização da Internet tem como baluartes o direito à liberdade de expressão e a constatação de que o aumento do fluxo de informação acessível satisfará, em certa medida, o interesse público[103].

É possível, ainda, falar de uma posição de corregulação da Internet que resultaria da interligação entre a lei e outros modos de regulação, num esforço para reconhecer a importância de uma simbiose entre as regulações pública e privada, de cariz comunitário e económico. De facto, esta posição aponta para a impossibilidade de um único agente regulador tomar posições sobre todos os assuntos relacionados com a Internet, dada a sua dimensão e a diversidade das questões jurídicas que levanta.

Parece que a solução aqui passará, mais uma vez, por uma situação de compromisso entre as duas posições, em que o autocontrolo, por parte dos utilizadores, através da filtragem de conteúdos, e da adoção, por parte dos fornecedores destes conteúdos, de códigos de conduta poderão ter um papel-chave, vendo a sua legitimidade reforçada quando apoiados pela lei estatal[104]. É preciso ter, no entanto, atenção a que uma legislação demasiado espartilhante poderá ter efeitos nocivos e revelar-se incapaz de acompanhar o processo de evolução das tecnologias e do mercado[105].

De resto, os próprios Estados já se encontram a influenciar o modo como o ciberespaço se tem desenvolvido, através da definição de linhas de fronteira entre a Internet e os demais meios de comunicação, e mediante uma regulação do comércio e dos conteúdos que vão circulando pela *web*, auxiliada por um controlo que se efetiva cada vez mais no aspeto técnico[106]. O chamado "Grupo de trabalho para a proteção das pessoas no que diz respeito ao tratamento de dados pessoais", previsto no artigo 29º da Diretiva n.º 95/46/CE[107], tem optado por não fazer distinções entre o mundo físico e o mundo virtual nas posições que tem tomado, sem, no entanto, deixar de levar em conta os condicionalismos desta realidade alternativa. Assim, os mesmos direitos definidos pela Diretiva em sede de proteção de dados

[103] Neste sentido, MARIA EDUARDA GONÇALVES, *Direito da Informação…,* ob. cit., p. 144.
[104] Cfr. MARIA EDUARDA GONÇALVES, *idem,* ob. cit., pp. 146 e 147.
[105] Veja-se GARCIA MARQUES, LOURENÇO MARTINS, *Direito da Informática…,* ob. cit., p. 430
[106] *Vide* MARIA EDUARDA GONÇALVES, *Direito da Informação…,* ob. cit., p. 148.
[107] O Grupo de protecção das pessoas no que diz respeito ao tratamento de dados pessoais (também conhecido por *Article 29 Working Party*), à luz do consagrado no artigo 29º da Diretiva 95/46/CE, tem funções consultivas e é independente, informando anualmente a Comissão Europeia sobre o estado de proteção dos dados pessoais respeitantes a cidadãos de dentro e de fora da União Europeia.

pessoais e, consequentemente, da vida privada (direito de acesso, retificação, informação e oposição) manter-se-ão, tendencialmente, a respeito dos intervenientes na Internet[108/109].

Por cá, esta intervenção legislativa mais direcionada para o tratamento de dados pessoais na Internet também se fez manifestar, valendo para estes casos as regras gerais previstas na Lei n.º 67/98, nomeadamente no n.º 4 do artigo 10º, que estipula que, em caso de recolha de dados em redes abertas, seja o titular dos mesmos informado de que os seus dados pessoais podem circular na rede sem condições de segurança, correndo o risco de serem vistos e utilizados por terceiros não autorizados. Aqui, merecem destaque os poderes de autoridade da CNPD, que lhe são conferidos, diretamente, pela alínea b) do n.º 3 do artigo 22º do mesmo diploma, e que a habilitam a "ordenar o bloqueio, apagamento ou destruição dos dados, bem como o de proibir, temporária ou definitivamente, o tratamento de dados pessoais, ainda que incluídos em redes abertas de transmissão de dados a partir de servidores situados em território português"[110].

Em suma, com a massificação de aparelhos informáticos, onde as diferenças entre um telemóvel e um computador estão cada vez mais esbatidas e onde o acesso à Internet se torna uma característica quase imprescindível, verifica-se uma descentralização das capacidades de recolha, tratamento e transmissão de informações pessoais[111]. Haverá, assim, que procurar uma conciliação entre as (inegáveis) virtudes da Internet[112] com a garantia das liberdades de expressão e de informação, bem como de outros valores impostos pela vigência de um Estado de Direito Democrático e que, como tal, são dignos de proteção por parte da ordem jurídica, procurando, ainda, tirar partido das potencialidades comerciais da rede[113].

3. A PROBLEMÁTICA DA TRANSMISSÃO E INTERCONEXÃO DE DADOS

Como temos vindo a observar, o número de recolhas e tratamentos de dados pessoais tem aumentado exponencialmente, fenómeno que se observa não apenas entre privados, dentro e fora do mesmo país, mas também entre administrações de diferentes Estados,

---

[108] Neste sentido, GARCIA MARQUES, LOURENÇO MARTINS, *Direito da Informática…,* ob. cit., pp. 425 e 426.

[109] Com efeito, uma Conferência que decorreu em Dublin a 23 e 24 abril de 1998, onde compareceram os comissários europeus de proteção de dados, veio reafirmar a extensibilidade das regulações europeias, no campo da proteção de dados, às atividades análogas realizadas no ciberespaço.

[110] A este respeito, CATARINA SARMENTO E CASTRO, *Direito da Informática…,* ob. cit., pp. 162 e 163.

[111] Cfr. MARIA EDUARDA GONÇALVES, *Direito da Informação…,* ob. cit., p. 87.

[112] Apesar de tudo, não poderemos negligenciar o papel fulcral que a Internet desempenha na formação e aprendizagem dos seus utilizadores, por toda a corrente de informação centralizada num único terminal que oferece, bem como pela variedade de serviços comerciais, culturais, de saúde, de comunicação e entretenimento que coloca à disposição.

[113] *Vide* MARIA EDUARDA GONÇALVES, *Direito da Informação…,* ob. cit., p. 143.

principalmente entre os Estados-membros da União Europeia (doravante, UE) e entre estes e países terceiros. Este fluxo materializou-se através da política de livre circulação de pessoas, mercadorias, serviços e capitais que pauta a atividade do mercado interno e, claro está, através do desenvolvimento dos meios de comunicação[114]. Com efeito, o fenómeno da informatização potenciou as possibilidades de cruzamento de ficheiros de dados de natureza pessoal, criando uma situação alarmante para os seus titulares que temem sofrer um tratamento abusivo ou discriminatório, quer por parte do Estado, quer por parte de entidades privadas[115/116].

Na verdade, apesar de existir um princípio geral que proíbe qualquer forma de transferência ou interconexão de dados pessoais automatizados, sejam estes de titularidade pública ou privada, este admite, contudo, algumas exceções consagradas na Lei n.º 67/98. Destaca-se, assim, o artigo 9º, onde se assinalam um conjunto de derrogações que passam pela comunicação prévia pelo responsável pelo tratamento à CNPD e a obrigatoriedade da conexão ser adequada à prossecução das finalidades e dos interesses legítimos destes mesmos responsáveis, sem que isso implique qualquer discriminação ou diminuição dos direitos, liberdades e garantias dos titulares, que deverão ser informados e consentir também em todo o processo. É, ainda, imperativo que sejam asseguradas todas as medidas de segurança, tendo em conta as especificidades dos dados em causa[117]. Só com a verificação cumulativa destes requisitos admite, a CNPD, a transmissão e interconexão de dados pessoais[118].

A questão adensa-se, sobretudo, quando envolve fluxos de dados transfronteiras, estando, igualmente, vedadas as transmissões de dados pessoais de um país para outro que não assegure as mesmas condições de segurança e um quadro legal equiparavelmente

---

[114] Neste sentido, CATARINA SARMENTO E CASTRO, *Direito da Informática…,* ob. cit., p. 306.

[115] Cfr. MARIA EDUARDA GONÇALVES, *Direito da Informação…,* ob. cit., p. 82. DANIEL J. SOLOVE, *The Digital Person: Technology and Privacy in the Information Age*, Nova Iorque e Londres, New York University Press, 2004, pp. 2 ss., fala mesmo na criação de "dossiers digitais" à medida que empresas e governos trocam informações sobre clientes e cidadãos para, assim, obter um conhecimento mais extensivo, diminuir riscos e melhor direcionar serviços.

[116] Quando o tratamento de dados pessoais seja realizado por entidade privada com quem o titular tenha vínculo contratual, terminada a ligação contratual entre ambos, a entidade, como responsável pelo tratamento, terá que proceder à destruição desses mesmos dados, salvo declaração em sentido oposto por parte do titular. Todavia, assegurando o responsável as condições de segurança necessárias, admite-se que estes dados possam ser conservados para lá da ligação contratual, como sucede no caso de listas tratadas automaticamente contendo informações que o titular forneceu e que são usadas para efeitos de publicidade e venda direta. A este respeito, CRISTINA QUEIROZ, *A Proteção Constitucional…,* ob. cit., pp. 307 e 308.

[117] *Vide* artigo 9º da Lei n.º 67/98.

[118] Esta questão foi abordada pelo legislador constitucional, nos n.ºs 2 e 4 do artigo 35º da CRP. GOMES CANOTILHO e VITAL MOREIRA defendem que a proibição da interconexão de ficheiros e bases de dados pessoais tem o propósito de combater o perigo da concentração de todos os dados pessoais de um cidadão numa única base de dados - remetendo para o perigo policial, uma vez que, através da interconexão de dados, a polícia teria acesso a meios privilegiados de controlo da vida dos cidadãos - e o perigo da multiplicação de ficheiros. Cfr. J. J. GOMES CANOTILHO, VITAL MOREIRA, *Constituição da República Portuguesa Anotada*…, ob. cit., p. 555.

responsável a assegurar um conjunto de princípios básicos e de garantias efetivas de proteção desses dados[119]. Estes requisitos encontram-se concentrados nos n.ºs 1 e 2 do artigo 19º da Lei n.º 67/98, pelo que, em todas as transferências autorizadas pela CNPD[120], terá que ser observada "a natureza dos dados, a finalidade e a duração do tratamento ou tratamentos projectados, os países de origem e de destino final, as regras de direito, gerais ou setoriais, em vigor no Estado em causa, bem como as regras profissionais e as medidas de segurança que são respeitadas nesse Estado".

A letra deste artigo poderá, no entanto, sofrer as derrogações previstas no artigo 20º do mesmo diploma, nunca sendo demais enfatizar a importância do papel do consentimento do titular dos dados e do papel da CNPD a conceder a autorização que apenas não poderá ir contra o previsto no n.º 5 do artigo 19º, que parece conferir a última palavra à Comissão Europeia, quanto à determinação da idoneidade de um país para que seja eventual destino de transmissão de dados pessoais[121].

De resto, convém frisar que a transferência de dados de natureza pessoal também poderá ocorrer na sequência de acordos ou convenções internacionais celebrados no escopo da UE[122], bem como fora deste âmbito, em casos tidos como mais extremos, como uma investigação judicial a nível global ou mesmo um intercâmbio de dados de natureza médica, necessários para o tratamento do titular em causa[123].

Especial relevância neste âmbito dos fluxos transfronteiras de dados assumem a Convenção para a Proteção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal, do Conselho da Europa[124] e, principalmente, a Diretiva n.º 95/46/CE, transposta para os ordenamentos jurídicos dos Estados-membros da UE.

---

[119] Um Estado, para que seja considerado idóneo a oferecer um nível adequado de proteção de dados pessoais, deverá enfatizar, na sua ordem jurídica, a existência de direitos, para os titulares desses dados, e de obrigações a quem procede ao seu tratamento. Estas regras deverão ser dotadas de eficácia prática, não se inibindo os Estados de acionar mecanismos processuais que assegurem o seu cumprimento. A este respeito, CATARINA SARMENTO E CASTRO, *Direito da Informática…,* ob. cit. pp. 283 e 284.

[120] *Vide* artigos 19º, n.º 3 e 20º, n.º 1 da Lei n.º 67/98.

[121] Igual entendimento têm GARCIA MARQUES e LOURENÇO MARTINS, *Direito da Informática…,* ob. cit., p. 363.

[122] Caso do acordo de Schengen ou da transmissão de informação relacionada com uma investigação levada a cabo pela Europol, por exemplo.

[123] Neste sentido, CRISTINA QUEIROZ, *A Proteção Constitucional…,* ob. cit., p. 307.

[124] Numa época em que a informatização dava, ainda, tímidos, mas decisivos passos, a Convenção para a Proteção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal (Convenção 108-1981) mostrou-se um elemento impulsionador na adoção de um quadro legislativo que encarasse com seriedade esta matéria nos países-membros, procedendo à sua harmonização. O modo flexível e facilmente adaptável ao desenvolvimento das novas tecnologias fez da Convenção um instrumento jurídico dotado de princípios que, ainda hoje, se revelam fulcrais para a proteção dos dados de natureza pessoal. Os princípios consagrados nesta Convenção tiveram repercussão na Diretiva n.º 95/46/CE, que seria aprovada anos mais tarde,

3.1. OS FLUXOS DE DADOS TRANSFRONTEIRAS NO ESCOPO DA DIRETIVA N.º 95/46/CE

Discute-se, ainda hoje, qual a verdadeira motivação por detrás da elaboração da Diretiva n.º 95/46/CE, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Para os autores GARCIA MARQUES e LOURENÇO MARTINS, bem como para CATARINA SARMENTO E CASTRO, o principal objetivo desta diretiva foi, na realidade, e ao invés do que a própria tenta fazer parecer (pela leitura do n.º 1 do seu artigo 1º), promover a circulação de dados pessoais entre os Estados-membros[125].

Não se quer, aqui, contudo, acusar a Diretiva de ter negligenciado o seu papel conformador no âmbito da proteção das liberdades e dos direitos fundamentais no que toca ao tratamento dos dados pessoais dos cidadãos[126], mas sim, apenas, evidenciar o facto das medidas por ela implementadas se destinarem a propulsionar o mercado único da Comunidade, que, caso contrário, veria o seu funcionamento comprometido, com os responsáveis pelos tratamentos a recusarem a sua transmissão para outros Estados-membros[127].

Com efeito, a Diretiva parece subalternizar a proteção dos indivíduos perante a ameaça da recolha e utilização indevida das suas informações pessoais, em função de uma flexibilização da circulação da informação, que resultaria numa harmonização tendente ao reforço do mercado interno e, consequentemente, ao progresso económico dentro da UE[128].

A Diretiva, ao ser transposta para o quadro legislativo interno dos Estados-membros, promove uma uniformização das regras de tratamento de dados de natureza pessoal com o mesmo nível de proteção[129], criando bases para que o fluxo de dados possa ser realizado sem

---

e tiveram o mérito de dar o primeiro passo no sentido de erradicar a existência de "paraísos de dados", bem como de estimular as transferências de informações através das fronteiras. Os esforços da Convenção 108-1981 foram concertados no sentido de conciliar o artigo 8º da Convenção Europeia dos Direitos do Homem, que concerne ao direito ao respeito pela vida privada e familiar, e o artigo 10º do mesmo diploma, respeitante à liberdade de expressão, na sua vertente de liberdade de informação. A este respeito, HERMINIA CAMPUZANO TOMÉ, *Vida Privada y Datos Personales...*, ob. cit., p. 79; GARCIA MARQUES, LOURENÇO MARTINS, *Direito da Informática…,* ob. cit., p. 265; IAN WALDEN, *Data Protection* in *Computer Law,* ob. cit., pp. 443 e 444.

[125] Cfr. CATARINA SARMENTO E CASTRO, *Direito da Informática…,* ob. cit., p. 276; no mesmo sentido, GARCIA MARQUES, LOURENÇO MARTINS, *Direito da Informática…,* ob. cit., p. 335.

[126] MANUEL HEREDERO HIGUERAS não se coíbe, no entanto, de acusar a Diretiva de querer eliminar o "travão" que a proteção das informações pessoais representa para a livre circulação dos dados na UE. *Vide* MANUEL HEREDERO HIGUERAS, *La Diretiva Comunitaria de Protección de los Datos de Carácter Personal,* Aranzadi Editorial, 1997, pp. 69 ss, *apud* GARCIA MARQUES, LOURENÇO MARTINS, *Direito da Informática…,* ob. cit., p. 334.

[127] A este respeito, CATARINA SARMENTO E CASTRO, *Direito da Informática…,* ob. cit., p. 276.

[128] Cfr. GARCIA MARQUES, LOURENÇO MARTINS, *Direito da Informática…,* ob. cit., pp. 333 ss.

[129] *Vide* Considerando 9 da Diretiva n.º 95/46/CE.

obstáculos, sem, no entanto, comprometer os direitos dos cidadãos que verão na mesma a sua privacidade assegurada, independentemente do Estado-membro que contenha informações a si respeitantes[130].

No entanto, a Diretiva, face ao desenvolvimento do comércio internacional, foi mais longe e ousou regular a transmissão de dados pessoais para países terceiros, ou seja, fora da UE. Dado que a Internet desafia, diariamente, a jurisdição dos Estados, só uma equiparação dos níveis de proteção dos dados pessoais fora da UE poderá assegurar a proteção dos dados pessoais dos cidadãos europeus[131].

A transferência de dados pessoais para países terceiros vem regulada no artigo 25º da Diretiva. Após uma breve análise a esta disposição, destaca-se a importância de existir um "nível de proteção adequado", que pressupõe a presença de um sistema efetivo de garantias capaz de salvaguardar os dados provenientes do país de origem nos países de destino[132]. É este o requisito base para que se possa encetar uma transferência de dados para um país terceiro, cabendo aos próprios Estados-membros comunicar entre si, e com a Comissão Europeia[133], se um determinado país terceiro não preencher os requisitos[134] para que possa ser considerado idóneo a ser destino de fluxos de dados pessoais.

---

[130] Cfr. CATARINA SARMENTO E CASTRO, *Direito da Informática…,* ob. cit., p. 276. GIUSEPPE CASSANO aponta um duplo objetivo da Diretiva no que toca à regulação em matéria de proteção de dados dentro dos países da UE: de um lado, evitar o vazio legislativo e, do outro, evitar uma disparidade de aplicações das normas que a transpõem. *Vide* GIUSEPPE CASSANO, *Dirito Dell'Internet, Il Sistema di Tutele della Persona, Milão,* Giuffrè Editore, 2005, p. 39.

[131] Neste sentido, MARIA EDUARDA GONÇALVES, *Direito da Informação…,* ob. cit., p. 175.

[132] A respeito da interpretação do artigo 25º da Diretiva n.º 95/46/CE, CATARINA SARMENTO E CASTRO - *Direito da Informática…,* ob. cit., pp. 278 ss -, convida-nos a olhar para o Acórdão do Tribunal das Comunidades Europeias de 6 de Novembro de 2003, já aqui referido, que veio delimitar, pela negativa, os contornos do que se entende por transferência de dados pessoais para países terceiros. No caso em análise, ocorrido na Suécia, uma catequista infringiu a lei de proteção de dados sueca ao disponibilizar, num *website* por si criado, e para promoção de atividades relacionadas com o seu trabalho para a Igreja Protestante da Suécia, informações pessoais relativas a dezoito colegas, sem o seu conhecimento e respetivo consentimento, não tendo sequer informado a autoridade de proteção de dados sueca. A questão que aqui se colocou, era a de saber se o caso em apreço perfilava uma situação de transferência de dados pessoais para um país terceiro. Ora, perante a ausência na Diretiva de qualquer definição do conceito de transferência de dados para países terceiros, e não tendo a Diretiva sequer estabelecido qualquer disposição especificamente direcionada para o uso da Internet, concluiu o Tribunal que "[n]ão existe uma «transferência para um país terceiro de dados» na aceção do artigo 25.° da Diretiva 95/46 quando uma pessoa que se encontra num Estado-Membro insere numa página Internet, de uma pessoa singular ou coletiva que alberga o sítio Internet no qual a página pode ser consultada e que está estabelecida nesse mesmo Estado ou noutro Estado-Membro, dados de carácter pessoal, tornando-os deste modo acessíveis a qualquer pessoa que se ligue à Internet, incluindo pessoas que se encontram em países terceiros".

[133] Como já vimos, a Comissão Europeia terá sempre a última palavra quanto a decidir pela idoneidade de um país terceiro para assegurar a proteção de dados pessoais. Veja-se o n.º 4 do artigo 25º da Diretiva 95/46/CE, disposição que tem o seu reflexo na ordem jurídica portuguesa no n.º 5 do artigo 19º da Lei n.º 67/98. Verifica-se, assim, que a Diretiva atribuiu um controlo especial à Comissão, quanto às transmissões de dados para países terceiros, reduzindo, consequentemente, a autonomia das autoridades de proteção de dados nacionais nesta matéria. A este propósito, MARIA EDUARDA GONÇALVES, *Direito da Informação…,* ob. cit., p. 106.

Não obstante, a Lei n.º 67/98 contempla, no seu artigo 20º, a possibilidade de Portugal transferir dados pessoais de cidadãos para países terceiros que não assegurem um nível adequado de proteção, verificadas as condições por esta norma impostas. Este artigo, na realidade, corresponde ao artigo 26º da Diretiva, onde se encontram as derrogações ao artigo 25º, que viemos a analisar. Daqui, destaca-se, para além das derrogações previstas no n.º 1 do artigo 26º, o disposto no n.º 2 do mesmo artigo, que acrescenta ser possível um Estado-membro autorizar a transferência de dados pessoais para um país terceiro que não ofereça um nível de proteção adequado, desde que o responsável pelo tratamento assegure garantias suficientes de protecção da vida privada e dos direitos e liberdades fundamentais das pessoas, assim como do exercício dos respetivos direitos, podendo essas garantias resultar de cláusulas contratuais adequadas, solução que tem sido fomentada pelos agentes económicos interessados.

Impera, aqui, que se encontre uma solução que possa harmonizar todos os interesses em jogo, nomeadamente o direito à reserva da intimidade da vida privada e à proteção dos dados pessoais dos cidadãos dos Estados-membros da UE, com os interesses económicos tendentes a um mercado internacional capaz de partilhar recursos, próspero e eficiente[135].

---

[134] Este nível de proteção adequado será avaliado "em função de todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados; em especial, serão tidas em consideração a natureza dos dados, a finalidade e a duração do tratamento ou tratamentos projetados, os países de origem e de destino final, as regras de direito, gerais ou sectoriais, em vigor no país terceiro em causa, bem como as regras profissionais e as medidas de segurança que são respeitadas nesse país." *Vide* n.º 2 do artigo 25º da Diretiva n.º 95/46/CE.

[135] A este respeito, cabe, aqui, uma referência ao Acordo *Safe Harbor* ("Porto Seguro"), realizado entre a UE e os Estados Unidos da América, com vista a ultrapassar as divergências em matéria de proteção de dados pessoais entre as duas potências económicas, que inviabilizavam a sua transferência. Com efeito, no âmbito dos n.ºs 5 e 6 do artigo 25º da Diretiva 95/46/CE, e mediante o disposto na Decisão n.º 2000/520/CE, desenvolveram-se determinados princípios - e diretrizes das questões mais frequentes (FAQ) - destinados a serem cumpridos pelas organizações norte-americanas aderentes, para que assim fosse assegurado um "adequado nível de proteção" dos dados pessoais transferidos de um Estado-membro da UE para os Estados Unidos da América, sem necessidade de garantias adicionais. A adesão a estes princípios é voluntária, sendo que a declaração de autocertificação deve ser enviada anualmente pelas organizações, sob pena de serem retiradas da lista de aderentes. Para maior desenvolvimento, CATARINA SARMENTO E CASTRO, *Direito da Informática…,* ob. cit., pp. 288 ss.; MARIA EDUARDA GONÇALVES, *Direito da Informação…,* ob. cit., pp. 181 e 182; DOMINGOS SOARES FARINHO, *Intimidade da Vida Privada…,* ob. cit., pp. 94 e 95.

II – EM ESPECIAL: O DIREITO AO ESQUECIMENTO

Se a autonomização do direito ao esquecimento, ou *the right to be forgotten*, - como novo direito destinado a proteger os dados dos utilizadores no ciberespaço - parece consistir num fenómeno relativamente recente, a verdade é que a premissa por que opera já vem sendo posta em prática há algum tempo, em variados ordenamentos jurídicos.

Este direito ao esquecimento, na sua fórmula mais primitiva, assume a forma de um direito que assiste aos ex-condenados - que já cumpriram a sua sentença e que se encontram em processo de reabilitação perante a sociedade - de impedirem a publicação dos factos por que foram sancionados, decorrido um certo período de tempo[136]. A razão aqui apresentada é a de que o interesse público sobre os ilícitos cometidos pelos criminosos em questão não tem uma duração ilimitada, devendo ser vedado o acesso aos registos, tendo decorrido sobre a condenação tempo suficiente[137]. Há, aqui, que sopesar, acima de tudo, uma ponderação entre o interesse do público em ter acesso à informação e o interesse do culpado que prossegue a sua reabilitação, na certeza, porém, de que, estando em jogo o interesse público dos cidadãos, não haverá lugar para a efetivação do direito ao esquecimento[138].

Ora, como temos vindo a observar, o direito ao esquecimento, na sua faceta estreitamente ligada à proteção de dados pessoais dos utilizadores na Internet, que aqui nos ocupa, é um direito moldado à imagem das novas tecnologias, procurando impor-se como um travão à coleta e processamento desenfreados de dados pessoais, ainda que fornecidos pelos próprios titulares, um problema que atingiu uma dimensão sem precedentes nesta era digital.

Este direito teve as suas raízes no ordenamento jurídico francês, onde é conhecido por *droit à l'oubli*. Com efeito, foi Nathalie Kosciusko-Morizet - à data, a Secretária de Estado francesa encarregue da pasta do desenvolvimento da economia digital - quem, através da elaboração de duas Cartas[139], abriu caminho para aquele que viria a ser o direito ao esquecimento desenvolvido pela Comissão Europeia, aqui em análise.

---

[136] *Vide* ROLF H. WEBER, *The Right to Be Forgotten: More Than a Pandora's Box?*, in JIPITEC, Vol. 2, 2011, pp. 120 e 121. Disponível em: http://www.jipitec.eu/issues/jipitec-2-2-2011/3084. No mesmo sentido, JEFFREY ROSEN, *The Right to Be Forgotten*, Stanford Law Review Online, 64, 13.02.2012, p. 88. Disponível em: http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-88.pdf.

[137] Este conceito é, ainda, por parte da jurisprudência, alvo de uma interpretação algo imprecisa.

[138] "O direito à informação prima quando os factos, mesmo íntimos, tenham relevo público". JOSÉ DE OLIVEIRA ASCENSÃO, *Direito Civil…,* ob. cit., p. 113.

[139] A *Charte sur la Publicité Ciblée et la Protection des Internautes*, assinada, a 30 de Setembro de 2010 e, sobretudo, a *Charte du Droit à l'Oubli dans les Sites Colaboratifs et les Moteurs de Recherche*, assinada a 13 de Outubro de 2010, por um grupo de representantes de redes sociais, operadores de motores de busca e outros

O direito ao esquecimento consiste, assim, num direito que tem por base a autonomia do titular dos dados pessoais de decidir o seu destino, após a sua colocação na Internet, visando dotar os cidadãos de um mecanismo que conte com a autoridade coativa da lei para lhes assegurar a faculdade de eliminar informações a seu respeito, na ausência de razões legítimas que justifiquem a sua manutenção, impedindo que estes dados caiam nas mãos de terceiros que deles poderão fazer um uso abusivo[140].

1. O DIREITO AO ESQUECIMENTO NO QUADRO LEGISLATIVO DA UE

Na Europa, o berço da hodierna proteção da privacidade, o direito ao esquecimento é, tradicionalmente, englobado nos direitos de personalidade que, como atentado *supra*, compreendem o direito à imagem, à honra e à reserva da intimidade da vida privada[141].

É - essencialmente - na Europa, usufruindo de um forte impulso por parte da UE, que se tem verificado uma maior intervenção na defesa da proteção de dados pessoais dos cidadãos, através da adoção de legislação nacional e comunitária[142], procurando disciplinar a atuação dos fornecedores de conteúdos que procedem ao tratamento das informações pessoais dos seus utilizadores[143].

A base jurídica para a atuação da UE no âmbito das relações do ciberespaço encontra-se no artigo 95º do Tratado da União Europeia, que se refere à necessidade de harmonização entre as legislações dos países membros, no sentido de concretizar o mercado interno. É aqui que encontramos o fundamento para as diretivas referentes ao comércio eletrónico[144] e à proteção de dados, sendo que, no caso desta última, se revela particularmente importante o

---

fornecedores de conteúdos *online*, no sentido de criar um código de conduta destinado a proteger os direitos dos utilizadores da Internet e os seus dados pessoais, na rede vertidos.É inevitável destacar a ausência da *Google* e do *Facebook*, que se recusaram a subscrever o diploma - HUNTON & WILLIAMS LLP, *French Government Secures "Right to Be Forgotten" on the Internet*, 21.10.2010. (Consult. 06.04.2012),
Disponível em: http://www.huntonprivacyblog.com/2010/10/articles/french-government-secures-right-to-be-forgotten-on-the-internet/.

[140] Em 2008, dois anos antes da Comissão Europeia ter anunciado as suas intenções de estabelecer um direito ao esquecimento, já JONATHAN ZITTRAIN tinha proposto um conceito análogo que denominou de *reputation bankruptcy*, pugnando por um *fresh start* para todos os que vissem a sua reputação comprometida na *web*. Veja-se, JONATHAN ZITTRAIN, *The Future of the Internet and How to Stop It*, New Haven e Londres, Yale University Press, 2008, pp. 228 ss.

[141] Cfr. ROLF H. WEBER, *The Right to Be Forgotten…,* ob. cit., p. 121.

[142] Em alguns países da Europa, *v.g.* na Holanda, estas iniciativas legislativas têm sido complementadas, pelas empresas, através da elaboração de códigos de conduta, resultando numa espécie de autorregulação destinada a conquistar a confiança dos utilizadores e dar um impulso à massificação do comércio eletrónico. *Vide* nota 122 de MARIA EDUARDA GONÇALVES, *Direito da Informação…,* ob. cit., p. 151.

[143] A este respeito, DOMINGOS SOARES FARINHO, *Intimidade da Vida Privada…,* ob. cit., p. 78.

[144] Diretiva n.º 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos jurídicos dos serviços da sociedade de informação, nomeadamente o comércio eletrónico, no mercado interno.

seu esforço em tornar possível a livre circulação destes dados, atribuindo-lhes um caráter económico[145].

Também no artigo 8º da Carta de Direitos Fundamentais da UE está expressamente prevista a proteção de dados pessoais, bem como no próprio Tratado de Lisboa, que remete para o artigo 16º do Tratado de Funcionamento da UE, e que, assim, lança as bases legais para a proteção de dados pessoais no âmbito de todas as atividades mantidas sob a alçada da UE[146].

Tradicionalmente, a Europa e os Estados Unidos da América (EUA) têm prosseguido políticas opostas em matéria de privacidade, com os EUA, como veremos, a optarem por uma abordagem mais liberal neste âmbito, orientada para um maior enfoque no desenvolvimento do empreendedorismo e prosperidade dos mercados e preterindo a proteção dos dados dos cidadãos. Embora ambos estejam de acordo que a proteção da privacidade dos consumidores de bens e serviços *online* é algo digno de salvaguarda, tal não parece ser prioritário para o legislador americano[147/148].

Apesar do significativo aumento na recolha de informações pessoais, apadrinhado pela expansão da Internet, VIKTOR MAYER-SCHÖNBERGER assinala um facto curioso. Na década de 90, após ter requerido às autoridades alemãs para a proteção de dados pessoais uma lista exaustiva de casos em que indivíduos processaram entidades que levaram a cabo recolha e tratamento dos seus dados pessoais sem o seu consentimento, deparou-se com a ausência total dos mesmos, facto que não se alterou substancialmente nos dias de hoje, mais de uma década depois, não apenas na Alemanha, mas em toda a Europa[149].

Na Alemanha, contudo, já está previsto o direito ao esquecimento referente à ocultação das identidades, em peças jornalísticas, de ex-condenados pela Justiça, uma vez

---

[145] Cfr. ANNIE BLANDIN-OBERNESSER, *L'Union Européenne et Internet*, Rennes, Editions Apogée, 2001, p. 29 *apud* MARIA EDUARDA GONÇALVES, *Direito da Informação…,* ob. cit., p. 149.

[146] *Vide* COMISSÃO EUROPEIA, *Commission Proposes a Comprehensive Reform…,* ob. cit.

[147] Neste sentido, EVA DOU, *Internet Privacy and the 'Right to Be Forgotten',* ob. cit. Para um estudo mais aprofundado nesta matéria, LUKAS FEILER, *Security Law in the EU and the U.S. – A Risk-Based Assessment of Regulatory Policies,* Viena e Nova Iorque, Springer, 2011.

[148] Uma das diferenças que mais se destacam entre as políticas de proteção de dados levadas a cabo entre a Europa e os EUA consiste na adoção dos sistemas de *opt-in* e de *opt-out*. Com efeito, na Europa, sempre prevaleceu o sistema de *opt-in*, que impede as empresas de reutilizar as informações pessoais dos seus clientes sem uma autorização expressa, por parte destes. Por sua vez, nos EUA, persiste um sistema de *opt-out*, em que, por defeito, se entende que o titular deu o seu consentimento para a reutilização dos seus dados, exigindo que seja o próprio a impedir tal situação - KENT LAWSON, *Online Reputation: What the Search Giants Know About You, Part 1*, 20.06.2011. (Consult. 18.03.2012). Disponível em: http://www.privatewifi.com/online-reputation-what-the-search-giants-know-about-you-part-1/.

[149] VIKTOR MAYER-SCHÖNBERGER, *Delete: The Virtue of Forgetting in the Digital Age*, Princeton e Oxford, Princeton University Press, 2009, pp. 83 e 84, procura explicar esta situação com o incómodo que tal significa para os titulares dos dados pessoais utilizados indevidamente, cumulado pela incerteza de uma decisão que, ainda que favorável, possivelmente, os exporá ainda mais (fenómeno conhecido por efeito *Streisand*).

paga a sua dívida perante sociedade[150]. Naquele país, é referência o caso célebre que, em 2009, envolveu Wolfgang Werlé e Manfred Lauber, que se tornaram conhecidos após terem assassinado, em 1990, Walter Sedlmayr, um ator alemão. Aquando da sua saída em liberdade condicional, os dois processaram, com sucesso, a enciclopédia *online Wikipedia*, na sua versão alemã, no sentido de verem retiradas as entradas nesta plataforma inseridas a seu respeito. O seu argumento foi, precisamente, o de que o Direito alemão acautelava estas situações, promovendo a reintegração na sociedade por parte de indivíduos em reabilitação, o que é, até certo ponto, verdade, uma vez que o Direito alemão lhes reconhece o "direito a serem deixados em paz". Esta situação e o consequente procedimento legal que se seguiu com o intuito de obrigar, também, a *Wikimedia Foundation* (empresa mãe que gere a enciclopédia) a remover as entradas, em língua inglesa, sobre si, colocou, novamente, em evidência, o fosso ideológico entre a tradição jurídica europeia e norte-americana quanto a esta matéria[151].

É, contudo, em Espanha, que o direito ao esquecimento tem reclamado maior atenção. Com efeito, recentemente, o governo espanhol decidiu agir, após cerca de 90 cidadãos terem submetido queixas à autoridade nacional para a proteção de dados, exigindo ao motor de busca *Google Search* que deixasse de exibir os resultados referentes às suas informações pessoais[152].

É, também, de assinalar que os modelos atuais do direito ao esquecimento não se têm mostrado propriamente intocáveis. Em Espanha e - novamente - envolvendo o *Google Search*, em abril de 2012, uma empresa ligada à construção de empreendimentos turísticos viu os seus esforços judiciais saírem gorados, com o tribunal a não dar provimento ao seu pedido para ver determinadas entradas naquele motor de busca removidas[153].

---

[150] Veja-se KENT LAWSON, *Do we need a Right to be Forgotten on the Internet?*, ob. cit.

[151] Cfr. JOHN SCHWARTZ, *Two German Killers Demanding Anonymity Sue Wikipedia's Parent*, in The New York Times, 12.11.2009. (Consult. 23.06.2012). Disponível em: http://www.nytimes.com/2009/11/13/us/13wiki.html; SUZANNE DALEY, *On Its Own, Europe Backs Web Privacy Fights*, in The New York Times, 09.08.2011. (Consult. 15.03.2012). Disponível em: http://www.nytimes.com/2011/08/10/world/europe/10spain.html?_r=2&%20sq=european%20privacy&st=cse&scp=1&pagewanted=all; LAWRENCE SIRY, SANDRA SCHMITZ, *Online Archives on Trial In Germany: Is there a Right to Be Forgotten?*, 2011, p. 5 e ss. (Consult. 23.06.2012) Disponível em: http://www.law.mmu.ac.uk/wp-content/uploads/2011/04/Online-Archives-on-Trial-in-Germany.pdf; SONYA ANGELICA DIEHN, *Spanish Firm Loses 'Right to Be Forgotten'*, in Deutsche Welle, 28.02.2012. (Consult. 23.06.2012). Disponível em: http://www.dw.de/dw/article/0,,15774283,00.html.

[152] Entre os queixosos, contam-se, inclusivamente, uma vítima de violência doméstica, levantando sérias questões de segurança, já que a sua morada podia tão facilmente ser obtida. O processo está, ainda, a decorrer nos tribunais espanhóis. Veja-se SUZANNE DALEY, *On Its Own, Europe Backs Web Privacy Fights*, ob. cit.

[153] O caso envolvia a intenção da empresa em ver eliminadas, dos resultados de pesquisa daquele motor de busca, fotografias com conteúdo sensível de um acontecimento que teve lugar naquele local, na década de 70, nomeadamente, envolvendo uma explosão de gás, na qual não teve qualquer envolvimento. A empresa alegava que tal prejudicava a sua imagem perante os clientes e, como tal, instava à *Google* que retirasse aquela entrada,

Por outro lado, o direito ao esquecimento tem no Governo francês um tenaz defensor, uma vez que foi neste ordenamento jurídico e na sua adoção do *droit à l'oubli* que se deram os primeiros passos para a implementação do direito ao esquecimento como hoje o concebemos. As Cartas[154] elaboradas para este propósito revelam-se, todavia, para alguns, como desprovidas de substantiva eficácia prática, apenas se destacando o apoio da *Microsoft France*, no que toca à obtenção da cooperação de grandes multinacionais[155].

Vozes contra a eventual efetivação do direito ao esquecimento, na formulação proposta pela Comissão Europeia, vêm, no entanto, por parte do Reino Unido, onde o Gabinete do Comissário de Informação tem manifestado a sua oposição, arguindo que tal trará implicações a nível da liberdade de expressão dos cidadãos europeus, iludidos por um direito impossível de assegurar[156].

De notar, ainda, que, no Reino Unido, onde também impera um sólido direito de liberdade de expressão, não existe um direito que assista aos cidadãos para que possam ver informação sobre si apagada[157]. Contudo, o *UK Data Protection Act*, bem como a Diretiva n.º 95/46/CE, garantem-lhes a possibilidade de aceder às informações sobre si detidas por terceiros, bem como de retificar as incorreções que delas constem[158].

Como pudemos observar, o direito ao esquecimento apresenta sérias dificuldades de efetivação, mesmo no continente europeu, onde encontra a sua maior base de apoio. A ausência de mecanismos que assegurem a sua eficácia e as potenciais implicâncias para a

---

algo a que o tribunal espanhol decidiu não aceder, entendendo que o papel da *Google* era ali, apenas subsidiário, não sendo o responsável direto pela existência das imagens. Veja-se SONYA ANGELICA DIEHN, *Spanish Firm Loses 'Right to Be Forgotten',* ob. cit.

[154] *Vide* nota 139 *supra.*

[155] A este respeito, STRUAN ROBERTSON, *Hasty Legislation Will Make a Mess of Europe's 'Right to Be Forgotten'*, in Out-Law, 12.11.2010. (Consult. 03.05.2012). Disponível em: http://www.out-law.com/page-11544.

[156] Esta posição é, inclusivamente, apoiada pelo próprio Ministro da Cultura britânico que alertou para a particular cautela que impõe a adoção de medidas legislativas quanto à sua praticabilidade, referindo que nenhum governo poderá assegurar que fotos partilhadas pela Internet poderão ser apagadas, na sua totalidade, e em todo o lado onde tenha havido acesso. O Ministro fez, ainda, questão de reforçar que afirmar a existência de um direito ao esquecimento é dar falsas expetativas aos cidadãos, questionando, também, a intenção da Comissão de submeter as empresas sediadas fora da UE ao seu quadro legislativo. Veja-se, BRIAN TARRAN, *'Right to Be Forgotten' is Unenforceable, says ICO*, in Research-Live, 17.11.2011. (Consult. 03.05.2012). Disponível em: http://www.research-live.com/news/government/right-to-be-forgotten-is-unenforceable-says-ico/4006419.article; BRIAN TARRAN, *The 'Right to be Forgotten' is a 'False Expectation'*, in Research-Live. (Consult. 03.05.2012). Disponível em: http://www.research-live.com/the-right-to-be-forgotten-is-a-false-expectation/4006392.blog.

[157] De referir, no entanto, uma decisão por parte do Tribunal Europeu dos Direitos do Homem, que sentenciou que a informação de ADN de pessoas consideradas inocentes não poderão ser armazenadas indefinidamente, o que obrigou o Reino Unido a rever a sua posição nesta matéria. VIKTOR MAYER-SCHÖNBERGER, *Delete: The Virtue of Forgetting…,* ob. cit., p. 83.

[158] Cfr. STRUAN ROBERTSON, *Hasty Legislation…,* ob. cit.

liberdade de expressão continuam a estar no epicentro das críticas, apesar da crescente onda de sensibilização para a preservação dos dados pessoais, neste paradigma da era digital, tão favorecida quanto assombrada pela omnisciência da Internet.

1.1. A NOVA PROPOSTA EM MATÉRIA DE DADOS PESSOAIS E DA SUA LIVRE CIRCULAÇÃO

Falar do direito ao esquecimento[159] no quadro legislativo da UE, implica falar da proposta, recentemente submetida a análise para o Parlamento Europeu e Conselhos de Ministros dos Estados-membros, por parte da Comissão Europeia (doravante, "nova proposta") [160]. Com efeito, a 25 de janeiro de 2012[161], VIVIANE REDING, Vice-Presidente da Comissão Europeia responsável pelas áreas da Justiça, Direitos Fundamentais e Cidadania, anunciou uma reforma no enquadramento legislativo reservado, atualmente, à proteção de dados pessoais na UE.

Esta reforma pauta-se, desde logo, por um objetivo de reforço da unicidade do mercado interno comunitário, tendo a Comissão Europeia, como *cheval de guerre*, a proteção dos dados pessoais dos utilizadores *online*, considerada uma autêntica moeda de troca no mercado digital dos dias de hoje e que, como tal, necessita de ser "estável e digna de confiança"[162].

VIVIANE REDING assume, assim, como prioritário, a promoção da UE como modelo a seguir no âmbito da proteção dos dados pessoais, uma vez que tal tornará a Europa muito mais competitiva, ao garantir a confiança tanto dos consumidores, como dos fornecedores de bens e serviços *online*. O silogismo realizado é o de que o aumento do sentimento de segurança e de uma maior disponibilidade dos cidadãos em fornecer os seus dados pessoais repercutir-se-á no fomento da economia digital, uma vez que, ao sentirem os seus dados

---

[159] O direito ao esquecimento encontra-se, especificamente, previsto no artigo 17º da nova proposta da UE relativa à proteção de dados pessoais e à sua livre circulação, que desenvolve e aprofunda o direito à retificação, apagamento ou o bloqueio dos dados pessoais já presente na alínea b) do artigo 12º da Diretiva n.º 95/46/CE. A nova proposta da UE encontra-se disponível em: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

[160] Uma vez aprovada, entrará em vigor passados dois anos.

[161] Na verdade, o anúncio não oficial da nova reforma reporta-se a uns dias antes, a 22 de janeiro de 2012, onde VIVIANE REDING, aproveitando a Conferência DLD (*Digital, Life, Design*) de Munique, revelou em primeira mão a iminência desta nova reforma envolvendo a proteção de dados pessoais na era digital. O discurso dessa conferência que, desde logo, absorveu algum do impacto dos críticos, está disponível em: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26.

[162] VIVIANE REDING, *The EU Data Protection Reform 2012: Safeguarding Privacy in a Connected World*, (discurso de apresentação da nova reforma), Bruxelas, 25.01.2012, p. 2. (Consult. 20.05.2012). Disponível em: http://ec.europa.eu/commission_2010-2014/reding/pdf/speeches/data-protection-reform2012_en.pdf. A este respeito, veja-se, também, JEF AUSLOOS, *The 'Right to Be Forgotten'…,* ob. cit., p. 10.

dignamente recolhidos e processados, continuarão a confiá-los a estas entidades. Estas, por sua vez, comprometer-se-ão a deles fazer um uso estritamente necessário à prossecução da sua atividade, dentro daquilo que lhes é imposto pelo enquadramento legislativo.

A Vice-Presidente da Comissão Europeia não deixou, contudo, de reforçar a sua crença nas possibilidades que as novas tecnologias representam para o desenvolvimento dos meios de comunicação e do comércio de bens e serviços na rede, apontando que, para que se possa tirar o maior partido destes expedientes, é necessário que haja uma regulação que os apreenda em toda a sua extensão e atente à sensibilidade das informações que a Internet movimenta[163/164].

Assim, de acordo com VIVIANE REDING, a nova reforma terá, a todo o momento, presente o princípio de que os dados pessoais pertencem sempre, e acima de tudo, ao seu titular, pelo que as políticas de privacidade terão de conter informações acessíveis ao cidadão comum, para que este se possa, constantemente, inteirar de quando os seus dados estão ou não a ser recolhidos e processados e possa fazer uma escolha informada sobre que dados revelar e a quem[165].

Neste sentido, surge o direito ao esquecimento e o poder, por este conferido aos respetivos titulares, de remoção dos dados pessoais inseridos no *website* de um fornecedor de conteúdos *online*. Com efeito, o considerando 53 da nova proposta refere que qualquer pessoa tem o direito a que os seus dados pessoais sejam apagados quando estes já não sejam necessários em relação ao motivo por que foram recolhidos e alvo de tratamento, quando tenham retirado o seu consentimento (ou nunca o tenham concedido) para que esses mesmos dados sejam processados, ou quando o tratamento dos seus dados não esteja de acordo com o postulado na nova proposta.

A nova proposta teve, ainda, a preocupação de estender o alcance do direito ao esquecimento *online*, ao estabelecer que os responsáveis pelo tratamento de dados pessoais

---

[163] Cfr. VIVIANE REDING, *idem*, ob. e loc. cits.

[164] Neste sentido, a proteção dos menores no ciberespaço foi também fortemente enfatizada no anúncio desta nova reforma legislativa (*vide* considerando 53 e n.º 1 do artigo 17º da nova proposta). Tal, vai de encontro ao intuito de possibilitar aos cibernautas a eliminação de algumas publicações (*v.g.* entradas de texto, ou mesmo a colocação de fotografias embaraçosas, num *blog* ou numa rede social), motivadas pela impulsividade da juventude e que, posteriormente, lhes poderão causar entraves aquando da sua chegada à vida profissional e a um mercado de trabalho cada vez mais competitivo e impiedoso. Cfr. VIVIANE REDING, *ibidem*, ob. e loc. cits.; no mesmo sentido, DANIEL J. SOLOVE, *The Future of Reputation…,* ob. cit, p. 17.

[165] A este propósito, VIVIANE REDING, *The EU Data Protection Reform 2012: Safeguarding Privacy…,* ob. cit., p. 3. No mesmo sentido, VIVIANE REDING, *The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age*, (discurso para a Conferência da DLD), Munique, 22.01.2012. (Consult. 20.05.2012).
Disponível em: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26.

(vulgo, as empresas que gerem os *websites*) que tenham tornado públicos os dados pessoais de utilizadores, deverão informar terceiros que tenham tido acesso a esses mesmos dados e os estejam também a processar, para que também estes procedam à sua remoção, bem como à de outras cópias que possuam[166].

Este direito não é, contudo, absoluto, sendo excecionado pela existência de razões legítimas que impeçam essa mesma remoção (não apenas do *website* acessível ao público, mas também da própria base de dados da entidade que o gere), relacionadas, como já observamos, com o interesse público em ter acesso à informação em causa[167/168]. No entanto, cabe, aqui, referir que o ónus da prova impenderá sobre os responsáveis pelo tratamento, competindo-lhes fazer prova das razões por detrás da sua necessidade de manter as informações do seu titular, ao invés de ser este a demonstrar o porquê de já não haver um interesse legítimo a suportar o armazenamento dos seus dados[169]. Por outro lado, também o consentimento, sempre que exigido para o processamento da informação, terá que ser dado pelo titular de forma explícita, não podendo este simplesmente ser assumido pelos responsáveis pelo tratamento[170].

A eventual implementação desta reforma tem sido, no entanto, posta em causa[171]. Para lhe dar coesão e fazer face à atual imprecisão legislativa[172], VIVIANE REDING pugna por um sistema que designa de *one-stop-shop*, em que a uniformização das medidas relativas à

---

[166] *Vide* considerando 54 e n.º 2 do artigo 17º da nova proposta. Este artigo prevê, ainda, que o responsável original pelo tratamento tome "todas as medidas razoáveis, incluindo medidas de ordem técnica" de modo a assegurar-se que a informação foi por si removida, bem como pelos terceiros que tenham publicado a mesma informação, sendo por ela responsável o controlador original quando tenha autorizado a estes terceiros a sua publicação.

[167] Neste sentido, VIVIANE REDING, *The EU Data Protection Reform 2012: Safeguarding Privacy…,* ob. cit., p. 4

[168] A própria proposta da Comissão Europeia prevê, no considerando 53, que os dados pessoais em questão possam não ser alvo do direito ao esquecimento, sempre que a sua manutenção for necessária por razões de caráter histórico, estatístico ou científico, bem como, por razões de interesse público nomeadamente, na área da saúde, de afirmação do direito à liberdade de expressão e, ainda, quando requerido por lei. Cfr. considerando 53 e n.º 3 do artigo 17º da nova proposta.

[169] A este propósito, leia-se MATT WARMAN, *Online 'Right to Be Forgotten' confirmed by EU*, in The Telegraph, 17.03.11. (Consult. 03.04.12). Disponível em: http://www.telegraph.co.uk/technology/internet/8388033/Online-right-to-be-forgotten-confirmed-by-EU.html.

[170] Veja-se COMISSÃO EUROPEIA, *Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses – press release*, 25.01.2012. (Consult. 22.02.12). Disponível em: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46.

[171] As críticas centram-se, essencialmente, num possível efeito nefasto que a reforma da UE poderá ter para as liberdades de expressão e de imprensa, como veremos *infra*.

[172] Alguns advogados têm vindo a salientar esta falta de uniformização legislativa, alertando para a impossibilidade de as grandes multinacionais cumprirem com as legislações atuais, em matéria de dados pessoais, em todos os 27 países da UE. Cfr. EVA DOU, *Internet Privacy and the 'Right to Be Forgotten'*, in Reuters, 17.03.2011. (Consult. 14.03.2012).
Disponível em: http://www.reuters.com/article/2011/03/17/us-eu-internet-privacy-idUSTRE72G48Z20110317.

proteção de dados pessoais pelo espaço comunitário permitirá que qualquer conflito possa ser resolvido pela autoridade de regulação para a proteção de dados pessoais do Estado-membro onde se localize a sede da entidade envolvida no litígio e responsável pela pretensa utilização abusiva de informações pessoais[173]. Desta forma, a empresa em questão terá apenas que cumprir o postulado numa única lei de proteção de dados, em vigor para todo o território da UE, e responder perante uma única autoridade de proteção de dados, uma vez que todas as congéneres, nos 27 ordenamentos, disporão de idênticos poderes para aplicar a lei, de forma efetiva[174], entre todos os Estados-membros, sendo irrelevante qual a autoridade que lide diretamente com o caso[175].

As mesmas leis serão, também, aplicadas a empresas estabelecidas fora da UE, desde que a sua área de ação também inclua o espaço comunitário e lidem com dados pessoais de cidadãos da UE[176]. Por outro lado, procurando não repetir o erro cometido aquando da elaboração da Diretiva n.º 95/46/CE, que não acautelou a expansão vertiginosa de uma Internet que dava então os primeiros passos, VIVIANE REDING tenciona dotar a nova reforma de longevidade suficiente (pelo menos, "trinta anos") e de terminologia adequada a acomodar novas tecnologias, mudanças nos mercados ou, mesmo, na opinião pública, uma regulação onde impere a versatilidade, sem comprometer a sua clareza quanto aos objetivos a que se propõe[177].

Assim, a - cada vez mais incontornável desatualização - propulsionada pelo desenvolvimento tecnológico da Diretiva n.º 95/46/CE, serviu de ponte para a consagração do direito ao esquecimento. De facto, com a massificação das redes sociais e do *cloud computing*[178], bem como da facilidade de transportar informação em inúmeros terminais (desde *smartphones* a *pen drives*), tornou-se imperativa a criação de uma legislação robusta,

---

[173] *Vide* VIVIANE REDING, *The EU Data Protection Reform 2012: Safeguarding Privacy…,* ob. cit., p. 4.

[174] Um dos grandes objetivos da proposta visa reforçar o papel das autoridades nacionais para a proteção de dados pessoais para que, consequentemente, se veja aplicada a lei com maior eficácia. Prevê-se, inclusivamente, que as autoridades ficarão encarregues de exercer o poder sancionatório face às entidades que não respeitem as regras impostas pela UE, o que poderá conduzir a sanções que poderão ascender a 1 milhão de euros, ou, mesmo, até 2% do volume de negócios anual por parte de uma dada empresa. *Vide* artigo 79º, n.º 6 da nova proposta; no mesmo sentido, COMISSÃO EUROPEIA, *Commission Proposes a Comprehensive Reform…,* ob. cit.

[175] Neste sentido, VIVIANE REDING, *The EU Data Protection Reform 2012: Making Europe…*, ob. cit.

[176] A este respeito, COMISSÃO EUROPEIA, *Why do we need an EU data protection reform?*, p. 2. Disponível em: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf; no mesmo sentido, COMISSÃO EUROPEIA, *Commission Proposes a Comprehensive Reform…,* ob. cit.

[177] A este respeito, MATT WARMAN, *EU Fights 'Fierce Lobbying' to Devise Data Privacy Law*, in The Telegraph, 9.02.2012. (Consult. 14.03.2012).
Disponível em: http://www.telegraph.co.uk/technology/internet/9069933/EU-fights-fierce-lobbying-to-devise-data-privacy-law.html.

[178] *Vide* nota 80 *supra*.

capaz de suportar o teste do tempo e adequada a proteger os dados pessoais dos cidadãos, onde o direito ao esquecimento poderá vir a assumir lugar de destaque.

2. O DIREITO AO ESQUECIMENTO FORA DA JURISDIÇÃO DA UE: O CASO DOS EUA

A abordagem das questões de privacidade dos cidadãos é, nos EUA, quase diametralmente oposta, em relação à orientação europeia. De facto, a ponderação daquele direito é, na esmagadora maioria das vezes, suprimida em função de um valor maior na sua tradição jurídico-política, o direito às liberdades de expressão e de imprensa. Na verdade, dos documentos legais fundadores da nação americana, incluindo a própria Constituição, não consta nenhuma disposição relativa a um direito à privacidade, pelo que apenas o *Federal Privacy Act*, datado de 1974, se reporta a esta questão, mas limitando-a, apenas, às informações pessoais recolhidas e processadas pelas agências federais norte-americanas, como o caso do *FBI* (*Federal Bureau of Investigation*)[179]. Assim, constata-se a ausência de qualquer mecanismo, com dignidade constitucional, que consagre um direito à autodeterminação informativa ao dispor dos cidadãos americanos para fazer face a qualquer invasão perpetrada por uma entidade exterior ao próprio Governo Federal[180]. Com esta sua política, o Governo norte-americano assume-se favorável à mais ampla livre circulação da informação, tanto no plano nacional, como internacional.

Contudo, não deixa de ser relevante salientar que, já por algumas ocasiões, se desenvolveram esforços no sentido de tomar uma posição quanto à inexistência de legislação federal nesta matéria, tendo sido, inclusivamente, debatidas no Congresso algumas propostas que não chegaram a ver a luz da promulgação. Tal rejeição poderá ser justificada pela ausência de apoio destas iniciativas legislativas por parte dos grandes grupos económicos, bem como pelo facto de serem alvo de uma forte resistência política, institucional e social[181]. Com efeito, os grandes grupos económicos, para quem se mostra vital ao desenvolvimento da sua atividade o tratamento das informações pessoais dos seus clientes, temem que uma regulação no plano da proteção dos dados pessoais possa vir a trazer graves perdas ao seu setor, movendo influências no sentido de que esta dinâmica permaneça inalterada nos

[179] DANIEL SOLOVE - *Digital Person…,* ob. cit., p. 62 -, contudo, alega que, apesar da palavra "privacidade" não estar plasmada no texto constitucional, esta não deixa de ser alvo da sua proteção, algo para que o Supremo Tribunal Federal terá contribuído ao moldar uma variedade de princípios constitucionais neste sentido.
[180] A este respeito, VIKTOR MAYER-SCHÖNBERGER, *Delete: The Virtue of Forgetting…,* ob. cit., p. 82.
[181] Cfr. MARIA EDUARDA GONÇALVES, *Direito da Informação…,* ob. cit., pp. 153 e 154.

próximos anos. A tudo isto, juntam-se, ainda, as dúvidas quanto à eficácia da adoção deste tipo de legislação[182/183].

Recentemente, no entanto, surgiram ecos de uma tentativa, por parte da Administração do Presidente Barack Obama, de regular a proteção dos dados pessoais dos utilizadores da Internet. A mudança de paradigma parece ser apoiada pelo Presidente da *Federal Trade Commission (FTC)*, agência com caráter independente, responsável por defender os direitos dos consumidores e a regularidade dos mercados, que admitiu já estar a agir contra empresas com políticas de privacidade falaciosas para os utilizadores[184].

Na verdade, foram os ataques terroristas de 11 de setembro de 2001 que ampliaram a tendência para uma recolha desenfreada de dados pessoais, colocando em foco a vulnerabilidade da privacidade dos norte-americanos. Os bancos passaram a recolher ainda mais dados relativos a transferências internacionais, no sentido de detetar operações de financiamento a grupos terroristas. Também as companhias aéreas, com voos para os EUA, têm, desde então, que fornecer, a uma miríade de agências de autoridade, informação detalhada sobre cada passageiro antes que o avião entre em espaço aéreo americano para que estas autoridades possam proceder a uma análise sumária de cada registo (que inclui moradas e informações bancárias) e o cruzem com bases de dados (tidas como pouco fiáveis) que contêm potenciais suspeitos de atividades com vista a prejudicar a nação americana. A estes, juntam-se, igualmente, os serviços de telecomunicações (aqui, à semelhança do que acontece na Europa) que são agora obrigados a proceder ao armazenamento dos registos das

[182] Neste sentido, VIKTOR MAYER-SCHÖNBERGER, *Delete: The Virtue of Forgetting…,* ob. cit. p. 83.

[183] Em 2008, WILLIAM STRAUS, Representante do Estado de Massachusets, elaborou um projeto de lei que visava permitir aos cibernautas optar por não verem monitorizada a sua atividade *online*, exigindo às empresas responsáveis que apagassem todos os dados relativos a essa atividade, para efeitos de marketing, decorridos 24 meses. Contudo, de imediato, as grandes empresas que dominam a publicidade na Internet, lideradas pela *Google*, se opuseram ao prosseguimento deste projeto, alegando a sua superfluidade e excessivo rigor. Cfr. KYLE CHENEY, GINTAUTAS DUMCIUS, *Internet Privacy Bill Stirs Concern Among Advertisers*, in Wicked Local, 08.07.2008. (Consult. 04.05.12).
Disponível em: http://www.wickedlocal.com/belmont/news/x390626994/Internet-privacy-bill-stirs-concern-among-advertisers#axzz1w14fAWV0; No mesmo sentido, VIKTOR MAYER-SCHÖNBERGER, *Delete: The Virtue of Forgetting…,* ob. cit., p. 85.

[184] A *FTC* tem, de resto, dado mostras de apoiar a implementação do sistema *opt-out* (*vide* nota 148 *supra*) no que toca ao rastreio dos movimentos dos utilizadores *online*. Veja-se DIANE BARTZ, *Obama Administration Seeks Internet Privacy Bill*, in Reuters, 17.03.2011. (Consult. 04.05.2012). Disponível em: http://www.reuters.com/article/2011/03/17/us-privacy-obama-idUSTRE72F83U20110317. Também a *Microsoft* se tem revelado um precioso aliado nesta mudança de paradigma - ainda que não acompanhada pela jurisprudência norte-americana - recebendo rasgados elogios por levar a cabo e apoiar, publicamente, a adoção de uma política de privacidade caraterizada por apenas manter as informações de caráter pessoal dos seus clientes apenas pelo tempo considerado necessário para a prossecução da sua atividade.

comunicações dos seus clientes, com o propósito de poderem vir a ser necessários no âmbito de uma investigação criminal[185/186].

Por tudo isto, surge dificultada a reunião de condições para que, num futuro próximo, a figura do direito ao esquecimento *online* possa integrar, eficazmente, o ordenamento jurídico norte-americano, tradicionalmente patrocinador de um direito à liberdade de expressão até às últimas consequências. Com efeito, o que se passa na prática, é que, salvo algumas raras exceções, se um *website* (ou órgão de comunicação social) tem informações sobre um determinado indivíduo, está autorizado a publicá-las, sendo que tal legitimidade lhe é concedida pela Primeira Emenda à Constituição dos EUA, o garante das liberdade de expressão, de imprensa, de culto, de reunião e de manifestação contra a autoridade pública[187]. Por outro lado, como já vimos, nem a *Bill of Rights* (que ampliou o texto constitucional), nem as dezassete emendas que se lhe seguiram consagraram qualquer garantia relacionada com o direito que assiste aos cidadãos de manter a sua vida privada[188].

Contudo, apesar de os direitos relacionados com a privacidade dos indivíduos não possuírem dignidade constitucional no ordenamento jurídico dos EUA, estes não deixam de ser uma parte importante da tradição jurídica americana. De facto, cabe-nos, aqui, relembrar o papel de dois advogados norte-americanos, SAMUEL WARREN e LOUIS BRANDEIS, já aqui mencionados, que, ao escreverem o famoso artigo *The Right to Privacy*, em 1890, foram os primeiros a pugnar pelo reconhecimento de um direito à reserva da intimidade da vida privada face à, até então inatacável, liberdade de imprensa.

Foi, de resto, a preciosa contribuição deste artigo que levou à criação daquela que poderá ser considerada como a figura mais próxima de um direito à privacidade no Direito

---

[185] Cfr. VIKTOR MAYER-SCHÖNBERGER, *Delete: The Virtue of Forgetting…,* ob. cit., pp. 83 e 84.

[186] Estas medidas encontram-se relacionadas com o postulado no modelo do Direito Penal do Inimigo *(Feindstrafrecht),* defendido por GÜNTHER JAKOBS, e que prevê a adoção de medidas de prevenção com o propósito de dar resposta às exigências de segurança por parte da sociedade, e que, ao mesmo tempo, poderão resultar numa limitação excessiva dos direitos, liberdades e garantias dos cidadãos. Para um estudo mais aprofundado nesta matéria, *vide* HÉLÈNE MARINE SERRA FERNANDES, *O Direito Penal do Inimigo: Reconfiguração do Estado de Direito?*, Dissertação de Mestrado em Direito (Área de Especialização em Ciências Jurídico Políticas), Porto, Faculdade de Direito da Universidade do Porto, julho 2011.

[187] A Primeira Emenda à Constituição dos Estados Unidos da América dispõe o seguinte: *Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.*

[188] Cfr. FRANZ WERRO, *The Right to Inform v. the Right to be Forgotten: a Transatlantic Clash*, in Center for Transnational Legal Studies Colloquium, Georgetown University, 05.2009., pp. 291 e 292. Opinião diferente tem, no entanto, DANIEL SOLOVE, que julga ver este direito consagrado nas "penumbras" das Emendas. Cfr. DANIEL J. SOLOVE, *The Digital Person…,* ob. cit., pp. 64 e 65.

norte-americano, a figura dos *privacy torts*[189], ou "delitos de privacidade", destacando-se, entre estes, o delito da divulgação pública de factos privados, ou *tort of public disclosure of private facts*. Segundo esta figura, os *media* podem ser responsabilizados pela publicação de factos, ainda que verdadeiros, referentes à vida privada dos indivíduos, quando tal se demonstre de sobremaneira ofensivo para a pessoa envolvida e quando esses factos não tenham interesse para o público[190].

Contudo, a eficácia desta figura desde sempre se mostrou aquém, ensombrada por um quase endeusamento da Primeira Emenda à Constituição e das liberdades de expressão e de imprensa nela postuladas[191].

Com efeito, em *Cox Broadcasting Corp. v. Cohn*[192], o Supremo Tribunal Federal norte-americano declarou como incongruente com a Primeira Emenda poder-se responsabilizar um órgão de comunicação social por publicar informações decorrentes de um registo público[193]. O Tribunal baseou a sua decisão no facto de a informação ter sido retirada de documentos acessíveis publicamente, dando lugar à presunção de que a informação em causa era de interesse público e, como tal, digna do escudo da Primeira Emenda[194].

Os casos que se seguiram na jurisprudência norte-americana trilharam, sensivelmente, o mesmo rumo, reforçando a impunidade dos *media* face à obtenção e divulgação de informações que contendam com a privacidade dos envolvidos. Em *Oklahoma Publishing Co. v. District Court*[195], o Supremo Tribunal Federal voltou a considerar um órgão da comunicação social como não responsável por ter divulgado informação a que teve acesso por ter assistido ao julgamento, devidamente autorizado pelo juiz. Desta forma, tais informações

---

[189] Os *privacy torts* decompõem-se, na realidade, em quatro figuras diferentes: *tort of intrusion upon seclusion* (que contende com a intrusão na esfera íntima do indivíduo), *tort of public disclosure of private facts*, *tort of false light* (relacionado com atos de difamação) e *tort of appropriation* (relacionado com a apropriação do nome de outrém para benefício próprio). Para maior desenvolvimento nesta matéria, DANIEL J. SOLOVE, *The Digital Person…,* cit., pp. 59 e 60. No mesmo sentido, DANIEL J. SOLOVE, *The Future of Reputation...*, ob. cit., pp. 119 ss.

[190] A este respeito, DANIEL J. SOLOVE, *The Digital Person…,* ob. cit., pp. 58-60. DANIEL SOLOVE alerta, ainda, para o facto desta figura estar mais vocacionada para lidar com invasões de privacidade perpetradas pela imprensa do que para dificultar os fluxos de informações pessoais de clientes entre empresas.

[191] *Vide* FRANZ WERRO, *The Right to Inform v. the Right to be Forgotten…,* ob. cit. p. 292.

[192] *Cox Broadcasting Corp. v. Cohn*, 420 U. S. 469, 493 – 496 (1975).

[193] Em causa estava uma ação judicial por invasão da privacidade intentada pelo pai de uma falecida vítima de violação contra a empresa de comunicação social, por esta ter publicado o nome da vítima aquando da cobertura do julgamento. Tal ia, inclusivamente, contra o *tort of public disclosure of private facts* previsto, também, no estado da Geórgia. Veja-se FRANZ WERRO, *The Right to Inform v. the Right to be Forgotten…,* ob. cit. p. 293.

[194] Cfr. FRANZ WERRO, *idem*, ob. e loc. cits.

[195] *Oklahoma Publishing Co. v. District Court*, 430 U. S. 308 (1977).

foram consideradas, novamente, como colocadas no domínio público, não podendo ser retiradas sem infringir, uma vez mais, a Primeira Emenda[196].

Por último, em *The Florida Star v. B. J. F.*[197], deu-se o caso de o Supremo Tribunal Federal reverter a decisão de um tribunal no Estado da Flórida que tinha considerado responsável um jornal local por ter publicado informações relativas a uma vítima de violação sexual, enquanto o suspeito se encontrava em parte incerta e a investigação ainda decorria[198]. Aqui a justificação para a mudança de posição por parte do Supremo Tribunal Federal foi algo diferente, baseando-se mais no facto de os interesses em jogo não justificarem amordaçar a liberdade de imprensa, sendo, assim, inconstitucional, proceder à sua responsabilização[199].

Como demonstrado, a jurisprudência nos tribunais norte-americanos tem vindo, quase invariavelmente[200], a entender que a publicação de informações sobre um determinado indivíduo, desde que verdadeiras, prevalece sobre qualquer direito que incida sobre a privacidade[201]. Parece, assim, claro que não há valorosos expedientes a que se possa recorrer para impedir que os *media* divulguem informação, quando obtida legalmente, resultando numa evidente apologia da Primeira Emenda à Constituição, que reforça a posição de que, enquanto não se registarem mudanças no paradigma que tem vindo a ser seguido pela jurisprudência, não haverá espaço para a implementação de um direito ao esquecimento no quadro legislativo norte-americano[202/203].

---

[196] Neste sentido, FRANZ WERRO, *The Right to Inform v. the Right to be Forgotten…,* ob. cit. p. 294.

[197] *The Florida Star v. B. J. F.*, 491 U. S. 524 (1989).

[198] Na verdade, a legislação na Flórida proibia a publicação do nome de vítimas deste tipo de crimes, mas, ainda assim, o jornal não se coibiu de divulgar o nome completo de B. J. F., após ter tido acesso a um relatório da polícia. *Vide* FRANZ WERRO, *The Right to Inform v. the Right to be Forgotten…,* ob. cit. pp. 295 e 296.

[199] Cfr. FRANZ WERRO, *idem,* ob. e loc. cits.

[200] De assinalar um caso passado no Estado da Califórnia, onde o Supremo Tribunal daquele Estado responsabilizou uma revista por ter publicado o passado de um ex-condenado reabilitado há onze anos, considerando que, apesar de poder haver algum interesse público na divulgação da história, a divulgação do nome da pessoa em questão pouco acrescentava quanto a este aspeto. *Vide* FRANZ WERRO, *The Right to Inform v. the Right to be Forgotten…,* ob. cit. p. 297.

[201] Neste sentido, KENT LAWSON, *Do we need a Right to be Forgotten on the Internet?,* ob. cit.

[202] A este propósito, FRANZ WERRO, *The Right to Inform v. the Right to be Forgotten…,* ob. cit. pp. 296 e 298.

[203] Dada esta inflexibilidade por parte da jurisprudência americana e a necessidade crescente por parte dos cidadãos de verem as suas informações pessoais a salvo, têm surgido, especialmente nos EUA, variadas empresas dedicadas ao *reputation management*, ou seja, à gestão da reputação dos cibernautas *online*. Estas empresas dispõem-se a "enterrar" nas profundezas da Internet quaisquer informações que possam ser prejudiciais à reputação dos seus clientes (adicionando novas entradas sobre estes para que figurem logo nas primeiras páginas dos motores de busca) ou, mesmo, contactando os *websites* para que retirem a informação, tudo pelo pagamento de uma quantia que pode ascender aos milhares de dólares. Estes serviços têm tido, na realidade, uma razoável taxa de sucesso. Cfr. DAVID LINDSAY, *EU Privacy Laws: The 'Right to Be Forgotten' is Not Censorship*, in Crikey, 21.02.2012. (Consult. .06.06.2012). Disponível em: http://www.crikey.com.au/2012/02/21/eu-privacy-laws-the-right-to-be-forgotten-is-not-censorship/.

Há quem especule que o Supremo Tribunal Federal norte-americano tenha perdido a noção da sua própria competência para determinar o que tem valor para o público ou não[204]. O que parece incontornável é que qualquer tomada de posição legislativa no ordenamento jurídico dos EUA terá, a todo o momento, que procurar desenlaçar a tensão entre o direito a uma autodeterminação informativa e os princípios constitucionais da liberdade de expressão e de imprensa, num esforço de compromisso que possa garantir a segurança de uma vida longe da exposição indesejada, sem que, no entanto, tal resulte numa mordaça exorbitada para os meios de comunicação social e os fornecedores de conteúdos na Internet, de tal modo que promova uma autocensura prejudicial aos próprios cidadãos e à democracia.

3. CONHECER O "INIMIGO"

3.1. REDES SOCIAIS: O FENÓMENO *FACEBOOK*

Ao longo deste trabalho, temos vindo a focar, com amiúde insistência, o papel da Internet na mudança do paradigma atual quanto à proteção de dados pessoais, através dos inúmeros serviços que nela encontraram uma sólida base de operações para a prossecução das suas atividades.

Ora, no caso das redes sociais, a Internet não se trata, apenas, de uma plataforma de atuação, afirmando-se, efetivamente, como condição indispensável à sua conceção e subsistência[205]. Na verdade, as redes sociais mais não são do que *websites* capazes de agregar indivíduos oriundos de qualquer parte do globo que, ao criarem o seu perfil (uma espécie de *doppelgänger* virtual), se colocam em permanente comunicação com os outros utilizadores da mesma rede, com os quais partilham interesses, rotinas, fotografia e vídeo, chegando, inclusivamente, a partilhar dados sensíveis entre si, como sejam opiniões políticas ou religiosas, o seu estado civil ou orientação sexual. As redes sociais mostram-se, assim, como um poderoso veículo de comunicação, mas a sua utilidade continua a ser ensombrada pelo facto de uma utilização irresponsável poder colocar em risco as informações pessoais não só dos utilizadores, mas de quem os rodeia[206].

---

[204] J. Q. WHITMAN, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 Yale L. J., 2004, pp. 1151 e 1204, *apud* FRANZ WERRO, *The Right to Inform v. the Right to be Forgotten…,* ob. cit. pp. 299 e 230.

[205] A respeito das redes sociais, veja-se DANIEL J. SOLOVE, *The Future of Reputation…,* ob. cit., pp. 24 ss.

[206] Recentemente, surgiram notícias da existência de empregadores que exigiam aos seus entrevistados as *passwords* das suas contas do *Facebook* para melhor aferirem a sua empregabilidade. A este respeito, ALEXANDRE MARTINS, *Empresas dos Estados Unidos Pedem Password do Facebook aos Candidatos a Emprego,* in Público, 26.03.2012. (Consult. 14.06.2012).

Figura de proa na "indústria" das redes sociais assume-se, então, o *Facebook*, rede social que, em março de 2012, contava com cerca de 901 milhões de utilizadores ativos[207]. Contudo, não só por ser a rede social com maior número de utilizadores, o *Facebook* se tem vindo a destacar, estando, nos últimos anos, no centro de variadas polémicas, quase todas envolvendo violações da privacidade dos seus utilizadores, cumuladas por uma gestão abusiva dos seus dados pessoais e por uma política de privacidade que se tem revelado, em certos aspetos, como letra morta.

Atentemos a situação, ocorrida em 2011, que teve, como protagonista, um estudante austríaco. Ao acionar uma opção presente no *website* desta rede social (apenas disponível para utilizadores europeus) que lhe permitia receber todas as informações que o *Facebook* detinha sobre si[208], desde o seu primeiro *log-in*, em 2008, Max Schrems deparou-se com uma realidade que serviria de alerta para muitos outros utilizadores e, sobretudo, para os *media* e para as autoridades de proteção de dados pessoais. Com efeito, foi-lhe remetido um CD-ROM que encerrava cerca de 1200 páginas contendo toda a sua atividade na rede social, incluindo pedidos de amizade, fotografias e mensagens privadas que o próprio já tinha apagado, correspondentes a três anos de atividade[209]. Ora, como observado *supra*, esta manutenção dos dados pessoais, por parte do *Facebook*, vai contra os ditames europeus nesta matéria, os quais consagram, na alínea e) do n.º 1 do artigo 6º da Diretiva n.º 95/46/CE, uma oposição à conservação ilimitada das informações pessoais dos utilizadores, referindo que esta manutenção apenas poderá ser realizada durante o período necessário para a prossecução das finalidades para que foram recolhidos os dados pessoais do utilizador ou para que são tratados posteriormente.

Max Schrems apercebeu-se, então, que não só a informação "capturada" por aquela rede social era muito mais do que aquela que antecipara, como a informação que julgara estar

---

Disponível em: http://www.publico.pt/Mundo/empresas-norteamericanas-pedem-dados-de-acesso-ao-facebook-aos-candidatos-a-emprego-1539453.

[207] Este número corresponde ao número de utilizadores ativos, mensalmente, naquela rede social, avançado pelo seu próprio gabinete de imprensa. *Vide* http://newsroom.fb.com/content/default.aspx?NewsAreaId=22.

[208] Note-se o artigo 12º da Diretiva n.º 95/56/CE que consagra o direito de acesso da pessoa em causa aos dados pessoais alvo de tratamento. De referir, contudo, que este direito de acesso não foi fácil de materializar, sendo necessárias 6 semanas e 23 e-mails para que o acesso aos seus dados pessoais lhe fosse facultado. Cfr. JULIA PRUMMER, *Max Schrems Não 'Gosta' do Facebook*, in Presseurop, 27.04.2012. (Consult. 14.06.12). Disponível em: http://www.presseurob.eu/pt/content/article/1881381-max-schrems-nao-gosta-do-facebook.

[209] A este respeito, COMISSÃO EUROPEIA, *How Will the Data Protection Reform Affect Social Networks?*, p. 1. (Consult. 25.02.2012).
Disponível em: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf. No mesmo sentido, *Estudante Processa Facebook*, 30.10.2010, (consult. 26.05.2012). Disponível em: http://www.youtube.com/watch?v=ObbiBeXevkE.

eliminada afinal permanecia nos seus servidores[210]. A sua indignação levou-o, inclusivamente, a criar uma organização denominada *Europe v. Facebook*, destinada a lutar contra as ofensas à privacidade perpetradas pelo *Facebook*, tendo já enviado para a autoridade de proteção de dados pessoais da Irlanda[211] - onde a empresa instalou a sua sede na Europa - cerca de 22 queixas neste sentido[212].

Na verdade, é a própria forma como o *website* é gerido e estruturado que instiga os utilizadores a fornecerem cada vez mais informação pessoal sobre si e sobre terceiros, através das inúmeras funções e *plug-in's* que a rede social oferece, como seja a sincronização com telemóveis e contas de correio eletrónico associadas, jogos e outras aplicações de entretenimento, e resultados de pesquisas efetuadas no próprio *website*. É assim que, alegadamente, o *Facebook* procede ao enriquecimento das suas bases de dados que se alargam a não utilizadores apanhados naquela teia de informação, abusivamente intercetada, já que o consentimento dos não utilizadores não é, em tempo algum, requerido, e a informação é obtida sem que disso se apercebam[213].

As críticas, contudo, não se ficam pelo tratamento e utilização abusivos dos dados pessoais promovidos pela empresa, destacando-se, ainda, as chamadas "listas inteligentes"[214] e o famigerado *timeline*, ferramenta que organiza cronologicamente a vida do utilizador desde que ingressou na rede social, tornando-se num "livro aberto" para a vida de cada um, e que, por defeito, está acessível a qualquer utilizador, proveniente da rede de amizade ou não[215].

Também do outro lado do Atlântico, nos EUA, as críticas têm ganho voz, com a *FTC* a dar seguimento às queixas que lhe chegaram e que culminaram num acordo entre o

---

[210] Veja-se COMISSÃO EUROPEIA, *How Will the Data Protection Reform Affect Social Networks?,* ob. cit. p. 1.
[211] Office of the Data Protection Commissioner.
[212] O grupo chamou, ainda, a atenção para o facto de o *Facebook* estar a proceder ao armazenamento de informação relativa a não utilizadores, sem qualquer tipo de consentimento da sua parte. Esta captura de informação pessoal de não-utilizadores é realizada, por exemplo, mediante a captura de e-mails, por intermédio de utilizadores, para envios de pedidos de adesão a não utilizadores, ou através da identificação, em fotografias constantes da página de utilizadores, de alguém que não o seja. Para um maior desenvolvimento, LAURA LOCKE, *Facebook Ireland Accused of Creating 'Shadow Profiles' on Users, Nonusers*, in Cnet News, 21.10.2011. (Consult. 15.06.2012). Disponível em: http://news.cnet.com/8301-1023_3-20123919-93/facebook-ireland-accused-of-creating-shadow-profiles-on-users-nonusers/?part=rss&subj=news&tag=2547-1_3-0-20.
[213] São os intitulados *shadow profiles*, ou "perfis-sombra". *Vide* LAURA LOCKE, *idem*, ob. cit.
[214] As "listas inteligentes" promovem uma maior divulgação de informação pessoal por parte dos utilizadores ao confrontarem-nos com formulários a respeito de variados aspetos da sua vida privada (a respeito da sua formação, emprego, estado civil, convicções religiosas e políticas, por exemplo), incentivando a uma maior exposição *online*.
[215] Outra polémica, de graves contornos, respeita às acusações, por parte da autoridade para a proteção de dados de Hamburgo, de que o *Facebook* é responsável por alojar ficheiros *cookies* nos computadores dos utilizadores que, inclusive, se mantêm ativos mesmo após estes encerrarem a sessão nas suas contas e mesmo que estas tenham, entretanto, sido apagadas.

Facebook e a *FTC*, segundo o qual a empresa se sujeitará a 20 anos de auditorias independentes, bem como à implementação de uma política de alterações nas configurações de privacidade do *website* apenas com o consentimento do utilizador[216].

Parece-nos, de uma forma algo paradoxal, que esta autoridade norte-americana encarou o problema com maior seriedade e eficiência. Com efeito, após as queixas submetidas por Max Schrems e a sua organização, a autoridade para a proteção de dados pessoais na Irlanda ordenou duas auditorias à sede europeia do *Facebook*. Contudo, realizadas estas diligências, e quando se supunha uma tomada de posição mais firme, eis que parece ter-se dado uma reviravolta dos acontecimentos. Destarte, a autoridade optou por uma posição de neutralidade, uma vez que ainda não tomou qualquer decisão oficial quanto à legalidade das práticas levadas a cabo pelo *Facebook*. Na realidade, até ao momento, a autoridade limitou-se a fazer recomendações que os responsáveis pela rede social não se dignaram a acatar[217].

Não é difícil de imaginar por que razão grandes empresas, como o *Facebook* e a *Google*, como veremos seguidamente, dedicam tantos esforços para proceder a uma maior recolha e a um certo grau de dificuldade (impossibilidade?) em permitir que os utilizadores apaguem os seus dados pessoais permanentemente. Tal é justificado, precisamente, pelo modelo de negócio prosseguido por estas empresas, e que se baseia na comercialização das informações referentes a outras pessoas, utilizadores ou não.

3.2. A "GERAÇÃO *GOOGLE*"[218]

Dada a praticamente infinita dimensão do ciberespaço, os motores de busca, desde sempre, se revelaram precioso auxílio na procura da mais recôndita informação acerca de virtualmente qualquer assunto. São indubitáveis as vantagens que os motores de busca

[216] Entre as críticas que chegaram à sede da *FTC*, destacam-se, novamente, o facto de o *Facebook* proceder à alteração das suas definições de privacidade sem obter o consentimento ou, tão pouco, informar os utilizadores da mudança; o acesso a dados pessoais dos utilizadores, supostamente *off-limits* por parte de empresas terceiras associadas (responsáveis pelas aplicações incorporadas na rede social); o facto de o *Facebook* partilhar as informações pessoais dos utilizadores com outras empresas para fins publicitários (apesar de ter prometido o contrário); a manutenção das contas dos utilizadores e da informação lá encerrada, mesmo depois de estas terem sido, supostamente, eliminadas; e o facto de não cumprir com o postulado no acordo de *Safe Harbor*, que regula a transferência de dados pessoais entre os EUA e a UE. Cfr. SARAH SHEARMAN, *Facebook* Settles With FTC Over Privacy Complaints, in BrandRepublic, 30.11.2011. (Consult. 16.16.2012). Disponível em: http://www.brandrepublic.com/news/1106970/Facebook-settles-FTC-privacy-complaints/.

[217] Questões político-económicas são aventadas para esta ausência de tomada de posição por parte da autoridade irlandesa para a proteção de dados pessoais, com o Governo irlandês a não se mostrar interessado em motivar uma possível saída do *Facebook* do território (e economia) irlandês, bem como da *Google* e *IBM*, duas outras multinacionais naquele país sediadas. *Vide* JULIA PRUMMER, *Max Schrems Não 'Gosta' do Facebook,* ob. cit.

[218] Expressão cunhada por DANIEL J. SOLOVE, *The Future of Reputation…,* ob. cit.

proporcionam, mas, como é geralmente apanágio do recurso à tecnologia, torna-se necessário perguntar que custos contrapesarão a comodidade que estas ferramentas oferecem.

Com a evolução dos sistemas de navegação no ciberespaço, os motores de busca tornam-se, também eles, alvo de um constante esforço de aperfeiçoamento, dotando-os, os seus programadores, de uma autêntica "inteligência artificial" capaz de ir beber informação não só aos tradicionais *websites*, como às redes sociais e a outras bases de dados de acesso público. Sem a ajuda destes utensílios, a tarefa de encontrar a informação desejada *online* seria hercúlea quando, na realidade, os motores de busca, coadjuvados por algoritmos capazes de eleger, por si próprios, os conteúdos mais relevantes, desempenham esta tarefa em décimos de segundo, sem "nada" cobrar por isso.

Se, no âmbito das redes sociais, a referência é o *Facebook*, no que tange aos motores de busca, o *Google Search* assume, claramente, o protagonismo, com cerca de mil milhões de pesquisas a serem efetuadas diariamente através das suas plataformas virtuais[219]. Contudo, a *Google*, hoje em dia, já não é apenas sinónimo do motor de busca de referência, mas sim, uma "marca" presente nos projetos tecnológicos mais vanguardistas e noutras ferramentas que usamos no nosso quotidiano[220].

Apesar de, atualmente, a empresa estar associada a inúmeras polémicas relacionadas com violações da privacidade e de manutenção abusiva de informações pessoais dos utilizadores, nem sempre esteve a *Google* do lado das ameaças à privacidade. Com efeito, a primeira das grandes controvérsias geradas em torno da empresa, em 2005, deveu-se, precisamente, à sua inflexível posição em ceder ao Governo americano os dados de pesquisas efetuadas pelos seus utilizadores, ao contrário de outros motores de busca que responderam afirmativamente a esta exigência[221]. O tribunal acabou por dar razão à *Google*, que alicerçou os seus argumentos na relação de confiança que gerou junto dos seus utilizadores e que seria,

---

[219] Veja-se, a este respeito, VIKTOR MAYER-SCHÖNBERGER, *Delete: The Virtue of Forgetting…,* ob. cit., p. 54. No mesmo sentido, DANIEL J. SOLOVE, *The Future of Reputation…,* ob. cit., pp. 9 ss.

[220] Como as plataformas *Gmail*, *YouTube*, os sistemas operativos *Android* (para telemóveis e *tablets*) e as aplicações *Google Maps* e *Google Street View*. Esta última já tinha sido alvo de contestação, na Alemanha, por ter recolhido fotografias de habitações sem autorização. Ainda no rescaldo desta polémica, novas preocupações foram levantadas, por parte de autoridades de proteção de dados pessoais europeias, acusando a *Google* de promover este serviço, não só com o propósito de recolher as imagens, mas também de coletar informações respeitantes às redes *wireless* das respetivas habitações. Para maior desenvolvimento, veja-se MATT WARMAN, *Online 'Right to Be Forgotten' confirmed by EU*, ob. cit.; COMISSÃO EUROPEIA, *How Will the EU's Data Protection Reform Strengthen the Internal Market*, p. 1. (Consult. 19.06.2012).
Disponível em: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/4_en.pdf.

[221] Efetivamente, estas ferramentas tornam-se um alvo extremamente atrativo para as grandes agências governamentais de informação, devido às informações acumuladas durante anos sobre os seus utilizadores, informações essas atualizadas automaticamente, de cada vez que uma nova pesquisa é efetuada.

imediatamente, comprometida, a partir do momento em que as suas informações pessoais fossem partilhadas com o Governo[222/223].

O zelo com que a empresa parecia querer gerir os dados pessoais dos seus utilizadores parece, no entanto, ter dado lugar a uma nova abordagem, menos delicada e menos preocupada em obter o seu consenso. Prova disso é a mais recente política de privacidade, adotada em março deste ano. Com efeito, desde essa data que os utilizadores de serviços *Google* (*Gmail, YouTube, Blogger, Google+*, entre outros) viram centralizadas as suas contas e respetivas informações, sem que, para tal, tenha sido pedido o seu consentimento e lhes tenha sido concedido um expediente *opt-out* ou um outro mecanismo que lhes permitisse preservar parte dos seus dados pessoais, a não ser deixar de usar qualquer serviço disponibilizado pela empresa[224].

As questões levantadas em torno da nova política de privacidade levaram, inclusivamente, os membros do *Article 29 Working Party*[225] a manifestar as suas "sérias dúvidas" sobre a legalidade da nova implementação e a aconselhar a *Google* a protelar a sua introdução, para que as implicações na privacidade dos seus utilizadores pudessem ser devidamente debatidas, algo a que a administração da empresa não acedeu[226].

Com efeito, está aqui em causa a criação de uma identidade única em todos os inúmeros serviços *Google*[227], destinada a obter um perfil mais completo de cada utilizador, para melhor direcionar a publicidade de que virá a ser alvo, colocando, também, grandes entraves à eventual aplicação de um direito ao esquecimento. Tal veio acicatar os ânimos no mais que evidente choque ideológico entre a empresa e a Comissão Europeia, com a sua Vice-Presidente, VIVIANE REDING, a deixar bem claro que pretende que a *Google* tome medidas no

---

[222] Cfr. VIKTOR MAYER-SCHÖNBERGER, *Delete: The Virtue of Forgetting…,* ob. cit., p. 93.

[223] Foi, na verdade, a mesma motivação que levou a empresa, em 2007, a proceder à implementação de uma política de colocação de prazos de validade nos dados de pesquisa dos utilizadores, que permitiu que as suas identidades fossem removidas, de forma automática, após um período de dois anos. *Vide* VIKTOR MAYER-SCHÖNBERGER, *idem*, ob. e loc. cits.

[224] Cfr. PETER BRIGHT, *Europe Proposes a Right to Be Forgotten*, in Ars Technica, 26.01.2012. (Consult. 20.06.2012). Disponível em: http://arstechnica.com/tech-policy/2012/01/eu-proposes-a-right-to-be-forgotten/.

[225] *Vide* nota 107 *supra*.

[226] Veja-se DAVID MEYER, *EU Puts Google Straight on 'Right to Be Forgotten'*, in ZDNet UK, 22.02.2012. (Consult. 20.06.2012). Disponível em: http://www.zdnet.co.uk/news/security/2012/02/22/eu-puts-google-straight-on-right-to-be-forgotten-40095097/.

[227] Na prática, esta centralização da informação dos utilizadores traduzir-se-á, por exemplo, no facto de os vídeos assistidos no *YouTube* moldarem os resultados das pesquisas no motor de busca, bem como a publicidade exibida a cada utilizador na sua conta de correio eletrónico *Gmail*. Para maior desenvolvimento, DAVID MEYER, *EU Justice Chief: Google is Playing Privacy Games*, in ZDNet UK, 02.03.2012. (Consult. 22.06.2012). Disponível em: http://www.zdnet.co.uk/blogs/communication-breakdown-10000030/eu-justice-chief-google-is-playing-privacy-games-10025538/.

sentido de promover a eliminação das informações pessoais dos utilizadores quando tal lhes seja requerido.

No centro desta polémica, está a distinção entre plataformas/serviços de alojamento *(hosting platforms)* e motores de busca, bem como a consequente posição legal a que os responsáveis de cada um ficam sujeitos. De facto, para a Comissão Europeia, o *Google Search* (bem como qualquer rede social) não é apenas uma plataforma de alojamento que, simplesmente, alberga o conteúdo sem proceder à sua organização e processamento e sem qualquer responsabilidade ou condicionamento por aquilo que é alojado, equiparando, tanto os motores de busca, como as redes sociais, a controladores de dados, que exercem controlo sobre o conteúdo que lhes é apresentado[228]. Já, para PETER FLEISCHER, responsável pelo departamento de privacidade da empresa, o *Google Search* é nada mais do que uma ferramenta ao dispor da comodidade dos seus utilizadores, limitando-se a encaminhá-los para conteúdos alojados noutros lugares da *web*. Como tal, entende que a responsabilidade por eliminar os conteúdos publicados *online* deverá caber, acima de tudo, a quem procede à sua publicação e não às plataformas onde os conteúdos se encontram alojados, e, muito menos, aos motores de busca que organizam e auxiliam na pesquisa de todos as informações publicamente acessíveis[229].

Outro argumento de peso continua a ser a dificuldade de controlo da cópia e republicação das informações. Esta grave contrariedade torna ainda mais delicada a tarefa dos *websites* em conseguirem que a informação que albergam (*v.g.* fotografias publicadas numa rede social) seja completa e permanentemente eliminada - tendo, para tal, que o exigir junto de terceiros que se tenham apoderado dos conteúdos - o que se poderá afigurar tecnologicamente impossível[230]. A Comissão, contudo, já veio esclarecer que aquilo que se

[228] Na verdade, *Google* e Comissão Europeia parecem divergir na própria definição de *hosting platfom*, uma vez que, para a empresa, estas plataformas não são mais do que serviços destinados a alojar conteúdo criado por utilizadores, aqui incluindo o *Facebook, YouTube* ou *Google+*, afirmando, mesmo, em conformidade com a eventual implementação de um direito ao esquecimento, que os utilizadores têm todo o direito de ver os dados inseridos nestes serviços apagados, se assim o desejarem. Desta sua definição de *hosting platform*, a empresa demarca o seu motor de busca, entendendo-o como mero expediente para apontar o caminho de conteúdos existentes noutros locais, sem quaisquer responsabilidades quanto ao conteúdo original. A Comissão, no entanto, e como já vimos, faz um entendimento mais aprofundado de *hosting platforms*, assumindo, tanto os motores de busca, como as redes sociais, como mais do que meras ferramentas de organização ou de alojamento de conteúdos, precisamente pelo controlo que exercem sobre as informações que veiculam. A este respeito, PETER FLEISCHER, *Our Thoughts on the Right to Be Forgotten*, in *Google* European Public Privacy Blog, 12.02.2012. (Consult. 16.05.2012). Disponível em: http://googlepolicyeurope.blogspot.pt/2012/02/our-thoughts-on-right-to-be-forgotten.html; DAVID MEYER, *EU Puts Google Straight on 'Right to Be Forgotten',* ob. cit.

[229] Cfr. PETER FLEISCHER, *Our Thoughts on the Right to Be Forgotten*, ob. cit.

[230] A este propósito, JEF AUSLOOS, *The 'Right to Be Forgotten'…,* ob. cit., p. 8.

impõe a estas plataformas, desde que tenham intervenção direta no processamento e reorganização dos conteúdos (caso específico dos motores de busca, ou mesmo das redes sociais, estas já como locais onde se encontra o conteúdo original) é que adotem as "medidas razoáveis, incluindo medidas de ordem técnica"[231], para que estes terceiros eliminem também as informações de que, ilegitimamente, se apropriaram, sendo, ainda, considerados responsáveis quando tenham, previamente, autorizado a publicação destes dados por terceiros. Para VIVIANE REDING, os motores de busca assumem, quanto a este propósito, um papel relevante, pois, uma vez que o utilizador decida eliminar o conteúdo publicado *online*, as plataformas de alojamento deverão, também, informar os motores de busca para que tais informações deixem de figurar nos resultados de pesquisa[232].

Também a este respeito, a *Google* se viu envolvida em contendas judiciais. Já atentamos *supra* alguns casos, ocorridos no ordenamento jurídico espanhol, tendo, num deles, a decisão sido favorável à empresa. A questão continua a ser largamente debatida quanto ao facto de os motores de busca serem ou não responsáveis pelos conteúdos que reúnem da Internet. Se o *Google Search*, e os outros motores de busca, devolvem qualquer responsabilidade para quem efetivamente publicou a informação *online*, vozes há que defendem que também os motores de busca deveriam ser chamados à colação[233].

Não obstante toda a controvérsia gerada, PETER FLEISCHER não deixa de atestar que a política de privacidade da empresa está de acordo com o postulado na Diretiva n.º 95/46/CE e na nova proposta da Comissão Europeia, asseverando que a *Google* prossegue a sua atividade segundo ideais de transparência e de respeito pela privacidade dos utilizadores, consagrando-lhes a possibilidade de remover informações pessoais que tenham publicado nalgum dos seus serviços[234/235].

A (necessária) conivência com a regulamentação europeia não impediu, contudo, a *Google*, de se revelar reticente quanto à implementação da nova proposta, tal como

---

[231] *Vide* nota 166 *supra*.

[232] Neste sentido, DAVID MEYER, *EU Puts Google Straight on 'Right to Be Forgotten',* ob. cit.

[233] Com efeito, alguns especialistas em questões relacionadas com a privacidade, como JAVIER DE LA CUEVA, alertam para o facto de, apesar de os motores de busca não serem os responsáveis pela publicação dos conteúdos, terem um papel fundamental na sua difusão, pelo que, sem o seu precioso auxílio, dificilmente seriam encontrados. *Vide* a este respeito, SUZANNE DALEY, *On Its Own, Europe Backs Web Privacy Fights*, ob. cit.

[234] PETER FLEISCHER não deixa, contudo, de salvaguardar que tal poderá não acontecer de forma instantânea, apresentando, como razões para esse atraso, a prevenção da eliminação de uma conta que tenha sido abusivamente invadida por outrem, bem como "razões de ordem legal e contratual". PETER FLEISCHER, *Our Thoughts on the Right to Be Forgotten*, ob. cit.

[235] Veja-se PETER FLEISCHER, *Our Thoughts on the Right to Be Forgotten*, ob. cit.. Esta possibilidade, resulta, aliás, do texto da política de privacidade, publicada no sítio oficial da *Google*, em: http://www.google.com/policies/privacy/.

apresentada pela Comissão Europeia, alegando que as novas regras não se encontram adequadas à realidade do *modus operandi* dos motores de busca, apesar de a Comissão assegurar que estes modelos de negócio foram, também, tidos em conta[236].

Ora, com a nova proposta legislativa à espera de ser implementada pela Comissão Europeia, empresas como a *Google* e o *Facebook* teriam, necessariamente, que pedir o consentimento aos seus utilizadores para que os seus dados fossem vendidos a terceiros com propósitos publicitários - o grande sustento destas empresas - e que, assim, encontraria um obstáculo a que estas empresas não estão habituadas e que comprometeria a fluidez de todo o processo, já para não mencionar das recusas, que, certamente, chegariam a números elevados.

Contudo, a posição da Comissão Europeia, reforçada pela eventual efetivação da nova proposta, mantém-se inflexível, atribuindo aos utilizadores a decisão consciente quanto a permitirem aos motores de busca e outros serviços a comercialização ou não das suas informações pessoais com terceiros. Nas palavras de VIVIANE REDING, *[t]he choice is not with the company, the choice is with the people, that is European Law*[237].

4. A PROTEÇÃO DOS DADOS PESSOAIS E A PROTEÇÃO DA "ECONOMIA DIGITAL", NA ÓTICA DO MERCADO ÚNICO

Como temos vindo a observar, a edificação de um mercado único foi, desde a sua criação, uma das prerrogativas da UE e das comunidades a que sucedeu. A concretização deste mercado único assentou em dois pilares que, cumulativamente, contribuíram para a sua viabilização, não obstante as barreiras inerentes a uma Europa unida, mas com divergências políticas, económicas e culturais, por vezes, acentuadas. Estes pilares são, na realidade, a garantia de liberdades de cariz económico - como as liberdades de circulação de bens, serviços, pessoas e capitais - e a harmonização dos quadros legislativos de cada país da União, de modo a tornar possível a operacionalidade deste mercado único e, consequentemente, o fomento da economia europeia[238/239].

---

[236] Como se sabe, a fonte de rendimento da empresa resulta da publicidade orientada para cada utilizador através das informações recolhidas, e agora centralizadas, sobre cada um, sendo que 97% da sua receita de 10 mil milhões de dólares, no último trimestre de 2011, resulta deste tipo de atividade. A este respeito, *EU Justice Chief Warns Google Over 'Sneaking' Citizens' Privacy Away*, ob. cit.

[237] VIVIANE REDING *apud EU Justice Chief Warns Google Over 'Sneaking' Citizens' Privacy Away,* ob. cit.

[238] *Vide* MARIA EDUARDA GONÇALVES, *Direito da Informação…,* ob. cit., p. 129.

[239] As preocupações com os direitos dos indivíduos também passaram a estar na ordem do dia. Desde cedo, se percebeu que, para que o comércio eletrónico fosse alvo de um processo de expansão, era necessário que fosse assegurada a proteção da vida privada dos indivíduos enquanto pessoas e na sua qualidade de consumidores, através da criação de estruturas que permitissem a realização de transações comerciais em segurança e sem

Ora, com o advento da Internet e das novas tecnologias de comunicação, tornou-se inevitável que esta economia europeia se convertesse, também, numa economia digital, passando muita da ação dos mercados a desenrolar-se em plataformas e serviços *online*.

Contudo, se, por um lado, foram os avanços tecnológicos que tornaram possível a própria conceção da economia digital, por outro, foi, novamente, a sua utilização irresponsável, aliada à avidez proporcionada pelas suas infindáveis possibilidades, que trouxeram as questões em torno da privacidade para a ordem do dia do comércio eletrónico[240].

De facto, com a crescente valorização das informações sobre os consumidores, os fornecedores de serviços têm vindo a desenvolver técnicas cada vez mais aprimoradas de cruzamento dos dados pessoais dos seus clientes, de modo a melhor traçarem o seu perfil de consumidores e, assim, lhes destinarem uma personalização de serviços (e publicidade) que vá de encontro àquilo que procuram[241].

É, paradoxalmente, o próprio cenário de progresso tecnológico quem acaba por desencorajar o desenvolvimento desta economia virtual. De facto, se confiar os dados pessoais a uma entidade terceira já se revelava um problema de proporções homéricas, a globalização das transmissões de dados e o fenómeno do *cloud computing* torna o controlo sobre as informações pessoais num desafio de maior dificuldade, inibindo a sua partilha e, como tal, a confiança na economia digital.

É esta confiança que a nova proposta da Comissão Europeia visa celebrar. Destarte, uma das prerrogativas da nova proposta passa, precisamente, pelo fortalecimento das relações entre consumidores e empresas *online*, numa ligação de benefício mútuo que assegure aos utilizadores condições para que realizem as suas transações através de plataformas virtuais, sentindo os seus dados pessoais (com especial relevo para as suas informações bancárias) alvo de um tratamento digno e apenas na medida do possível a tornar possível o negócio em causa.

Mas nem só o sentimento de insegurança quanto à proteção das informações pessoais dos consumidores se tem imposto ao desenvolvimento da economia digital. Com efeito, um outro grande obstáculo à sedimentação desta economia prende-se, não podemos deixar de realçar, com o facto de haver uma divergência nos quadros legislativos, e na consequente aplicação das leis de proteção de dados pessoais dentro do próprio território da UE, resultante do modo como a Diretiva n.º 95/46/CE foi transposta para os respetivos ordenamentos

---

comprometer a intimidade dos utilizadores dos serviços *online*. A este respeito, HERMINIA CAMPUZANO TOMÉ, *Vida Privada y Datos Personales…,* ob. cit., p. 57.

[240] A este respeito, JEF AUSLOOS, *The 'Right to Be Forgotten'…,* ob. cit., p. 10.

[241] Cfr. MARIA EDUARDA GONÇALVES, *Direito da Informação…,* ob. cit., p. 173.

jurídicos dos 27 Estados-membros. Ora, este panorama de incerteza legal não se afigura favorável para as empresas que operam dentro da comunidade, gerando dificuldades óbvias ao desempenho da sua atividade e, mesmo, uma proteção desigualitária para os cidadãos e consumidores[242].

Também para esta questão a nova proposta da Comissão Europeia procura encontrar uma solução que passará, como já vimos, pela uniformização de um quadro legislativo em matéria de proteção de dados pessoais que traga de volta uma estabilidade legal que comprometa os mercados, e seus intervenientes, e nela se possam basear[243].

Vozes críticas não tardaram, contudo, a levantar-se face a esta nova proposta e ao impacto perverso que auguram vir a ter a sua implementação para a economia digital que tanto se preocupa em revitalizar.

Com efeito, a primeira grande questão colocada pelos detratores da nova proposta, prende-se com o facto da implementação de um sistema *opt-in*, quanto ao uso das informações dos consumidores, vir a diminuir drasticamente as possibilidades de recolha de informação, por parte das empresas, que fazem da comercialização destes dados o seu principal sustento[244].

Também por parte de órgãos oficiais de ordenamentos jurídicos como o Reino Unido, a questão foi abordada com cautela. A Câmara Internacional de Comércio, na sua dependência britânica, e na pessoa do seu anterior CEO, Stephen Pattinson, reforçou a necessidade de se apreender todo o alcance proposto por esta reforma, lembrando que é necessário ter em conta os custos que a sua implementação acarretará para as empresas, no

---

[242] *Vide* COMISSÃO EUROPEIA, *How Will the EU's Data Protection Reform Strengthen the Internal Market,* ob. cit. p. 1.

[243] Desta forma se prevê a aplicação de uma única lei a todas as empresas que operem dentro do território da comunidade, renunciando a despesas administrativas dispensáveis e que a Comissão Europeia estima que se situem na ordem dos 2,3 mil milhões de Euros, por ano, para as empresas. Os números não se ficam por aqui e a Comissão prevê, ainda, uma desburocratização do sistema que venha a trazer uma poupança de cerca de 130 milhões de Euros, por ano. É objetivo da Comissão promover uma maior responsabilização por parte dos controladores de dados, ao impor, como contrapartida, a estas entidades, rigorosos deveres de vigilância. Entre estes, destaca-se o dever de notificar as autoridades nacionais de qualquer fuga de informação de que tenham sido alvo, se possível, num período de 24 horas, estando, ainda, prevista, a obrigatoriedade de nomeação de um "agente de proteção de dados" independente, responsável por zelar pelo cumprimento de todos os ditames nesta matéria, nas empresas com mais de 250 funcionários. A este propósito, COMISSÃO EUROPEIA, *New Rules: New Benefits for Business.* (Consult. 23.06.2012). Disponível em: http://ec.europa.eu/justice/data-protection/minisite/business4.html; COMISSÃO EUROPEIA, *Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses,* ob. cit.

[244] Neste sentido, vários *websites* fornecedores de serviços *online* já alertaram para um possível fim dos serviços gratuitos que estes colocam à disposição dos utilizadores (a começar pelas plataformas de correio eletrónico), uma vez que, perdendo a sua principal fonte de receitas, só começando a cobrar pelo serviço prestado poderiam sobreviver.

sentido de não funcionar como um travão ao investimento na inovação tecnológica e nos próprios modelos de negócio. Stephen Pattinson mostra-se cético quanto ao pretenso equilíbrio apresentado pela proposta da Comissão, colocando o foco na recolha dos dados dos consumidores para o desenvolvimento de novos serviços, para que a proteção da privacidade de cada um não asfixie um dos maiores dinamizadores da competitividade e crescimento económico[245/246].

Levando em conta todo o disposto, parece-nos que os modelos de negócio *online* se deverão conduzir segundo um ideal de "privacidade por defeito", conseguido recorrendo ao auxílio de meios técnicos[247], mantendo como prioritárias, durante todas as fases do seu desenvolvimento - a começar na sua conceção - as preocupações com a proteção dos dados pessoais dos consumidores, independentemente do ramo de comércio em que pretendam transacionar[248].

Não obstante, e por tudo, o que temos vindo a acompanhar até aqui, a inclusão de um botão de *delete* parece continuar a não fazer parte dos planos de construção dos novos négocios *online*, que continuam a não se poder dar ao luxo de desaproveitar a sua fonte vital de financiamento, os dados pessoais dos seus clientes.

5. A PROTEÇÃO DE DADOS PESSOAIS E A PROTEÇÃO DAS LIBERDADES DE EXPRESSÃO E DE IMPRENSA

Das objeções que assolaram a eventual implementação de um direito ao esquecimento, propugnada pela recente proposta da Comissão Europeia, rapidamente se destacaram as críticas direcionadas pelos paladinos da liberdade de expressão, alarmados que tal expediente possa resultar num clima de censura, servindo-se da privacidade como um alibi de útil credibilidade[249]. Estas críticas suportam-se na ambiguidade de que é acusado este direito, pelo

[245] *Vide* MATT WARMAN, *Digital 'Right to Be Forgotten' Will Be Made EU Law,* ob. cit.

[246] Também não é de arredar a hipótese de serem os próprios governos europeus a responder às críticas por parte dos controladores de dados, rendendo-se ao espetro da crise económica que assola a Europa, e se oponham à implementação da nova proposta e aos seus efeitos para a economia digital.

[247] A propósito da utilização destes meios técnicos, é digna de destaque a proposta de VIKTOR MAYER-SCHÖNBERGER, que consiste na introdução de "prazos de validade" nos ficheiros com informações pessoais criados pelos utilizadores/consumidores, que seriam destruídos automaticamente ultrapassado este prazo. Mas também este sistema se afigura como insuficiente, dadas as apuradas técnicas de circunvenção já existentes. Para maior desenvolvimento, VIKTOR MAYER-SCHÖNBERGER, *Delete: The Virtue of Forgetting…,* ob. cit., pp. 90 ss.

[248] A este respeito, COMISSÃO EUROPEIA, *How Will the EU's Data Protection Reform Benefit European Businesses?*, ob. cit., p. 2.

[249] Nas palavras de PETER FLEISCHER, *[p]rivacy is the new black in censorship fashions. It used to be that people would invoke libel or defamation to justify censorship about things that hurt their reputations. But invoking libel or defamation requires the speech not be true. Privacy is far more elastic, because privacy claims can be made*

menos até à sua efetivação, temendo-se que abra as portas a uma remoção desenfreada do conteúdo partilhado na Internet, tanto pelos seus utilizadores comuns, como pelos órgãos de comunicação social.

É perigoso cair na tentação de encarar esta questão como uma competição entre a proteção de dados pessoais com o direito à informação e o direito a ser informado. A censura será sempre um espetro inquietante no horizonte de qualquer cidadão num Estado de Direito Democrático consciente dos seus direitos, pelo que a manutenção da privacidade, ou do direito à autodeterminação informativa, poderá, efetivamente, colocar-se em conflito com outros direitos, nomeadamente o direito à liberdade de expressão associada à utilização livre de recursos disponibilizados na Internet[250]. Para EUGENE VOLOKH, a explicação para este conflito parte da dificuldade do direito à autodeterminação informativa, "o direito de controlar o que os outros dizem sobre nós", implicar que seja o Estado quem impede a circulação dessa mesma informação[251].

É um facto que os direitos à liberdade de expressão e à liberdade de imprensa nunca foram revestidos de um caráter absoluto, apesar de estarem consagrados em diplomas nacionais e internacionais como direitos fundamentais[252]. Vemos, inclusivamente, que estes direitos estão dotado de uma genética flexível, sendo alvo de restrições quando sejam trazidos à colação direitos de outrem, desde que legítimos, ainda que sempre protegidos por um omnisciente princípio da proporcionalidade, norteado pelo interesse público[253]. Ora, se estas limitações se aplicam no mundo dito *offline*, não se vislumbra por que não hão-de ser, também, aplicadas, ressalvando-se as necessárias adaptações, ao contexto da Internet, onde a divulgação da informação prolifera a uma velocidade e com um alcance sem precedentes.

---

on speech that is true. PETER FLEISCHER, *Foggy Thinking About the Right to Oblivion*, 09.03.2011. (Consult. 22.06.2012). Disponível em: http://peterfleischer.blogspot.pt/2011/03/foggy-thinking-about-right-to-oblivion.html.

[250] Neste sentido, JOÃO PALMEIRO, *O Direito ao Esquecimento*, in Setúbal na Rede, 23.05.2011. (Consult. 23.06.2012). Disponível em: http://www.setubalnarede.pt/content/index.php?action=articlesDetailFo&rec=14802; L. GORDON CROVITZ, *Forget Any 'Right to Be Forgotten'*, in The Wall Street Journal, 15.11.2010. (Consult. 23.06.2012). Disponível em: http://online.wsj.com/article/SB10001424052748704658204575610771677242174.html.

[251] Veja-se EUGENE VOLOKH, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000), p. 2.

[252] O artigo 37º da CRP consagra não só a liberdade de expressão aos cidadãos, bem como o direito de informar, de se informar e de ser informado. Por seu lado, a liberdade de imprensa está assegurada nos artigos 38º e 39º da Lei Fundamental. *Vide*, ainda, artigo 10º da Convenção Europeia dos Direitos do Homem.

[253] O próprio n.º 2 do artigo 10º da Convenção Europeia dos Direitos do Homem admite restrições à liberdade de expressão, posto que estas sejam "necessárias, numa sociedade democrática, para a segurança nacional, a integridade territorial ou a segurança pública, a defesa da ordem e a prevenção do crime, a proteção da saúde ou da moral, a proteção da honra ou dos direitos de outrem, para impedir a divulgação de informações confidenciais, ou para garantir a autoridade e a imparcialidade do poder judicial".

Ao longo deste trabalho, temos vindo a defender a atribuição de um maior controlo dos dados pessoais aos seus titulares, de forma a evitar que estes sejam utilizados sem o seu consentimento e de forma abusiva, para finalidades diversas daquelas que justificaram a sua recolha. Com efeito, a atribuição de uma maior autoridade aos indivíduos no controlo dos seus dados pessoais resulta numa maior inibição da sua recolha, tratamento, armazenamento e posterior utilização ou divulgação por parte dos controladores, o que, para aqueles que se dedicam à publicação de conteúdos informativos (de utilizadores comuns, a redes sociais ou a órgãos de comunicação social) se perfila como uma clara violação das liberdades de expressão e de imprensa.

Assim, se os primeiros ecos das críticas já se faziam ouvir em novembro de 2010, aquando do primeiro anúncio da Comissão Europeia quanto a uma iminente reforma no âmbito da proteção de dados pessoais[254], estes intensificaram-se, mais recentemente, com o efetivo surgimento da proposta. JEFFREY ROSEN, uma das vozes que mais alto entoaram contra o direito ao esquecimento, referiu-se a este direito como "a maior ameaça à liberdade de expressão na Internet da próxima década"[255], acusando a proposta de promover um fosso ideológico ainda mais acentuado entre a Europa e os EUA, ao nível do equilíbrio entre a privacidade e a liberdade de expressão.

Mesmo reconhecendo os problemas inerentes a uma era digital que em tudo dificulta uma evasão ao passado, JEFFREY ROSEN acredita que a Comissão Europeia negligenciou o impacto deste direito quanto à liberdade de expressão dos cibernautas[256], apoiando-se, inclusivamente, em PETER FLEISCHER, já aqui amplamente referenciado, para expor as suas preocupações. Com efeito, no seu *blog*, PETER FLEISCHER procedeu a elencar três situações distintas em que o direito ao esquecimento possa contender, progressivamente, com a liberdade de expressão[257], situações essas que JEFFREY ROSEN se dispôs a analisar.

A primeira conjuntura, que se apresenta como a menos controversa, diz respeito ao direito de que cada um dispõe quanto a ver eliminado da Internet algo que o próprio tenha publicado, como seja, a título de exemplo, uma publicação numa rede social. A este quadro, tanto JEFFREY ROSEN como PETER FLEISCHER, não se mostram avessos, considerando, no

[254] Atente-se COMISSÃO EUROPEIA, *European Commission Sets Out Strategy to Strengthen EU Data Protection Rules*, 04.11.2010. (Consult. 28.06.2012).
Disponível em: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1462.
[255] JEFFREY ROSEN, *The Right to Be Forgotten*, ob. cit., p. 88.
[256] A este respeito, JEFFREY ROSEN, *idem*, ob. e loc. cits.
[257] *Vide* PETER FLEISCHER, *Foggy Thinking About the Right to Oblivion*, ob. cit.

entanto, que tal direito já existe e é, de resto, respeitado pela maioria dos controladores de dados pessoais, servindo, quando muito, para imbuir de uma maior responsabilidade estas entidades, no sentido de que efetivamente cumpram aquilo que anunciam e procedam à eliminação dos conteúdos, a pedido do seu titular[258].

Se esta situação se demonstra pacífica, tanto para os defensores da liberdade de expressão, como para os defensores da implementação de um direito ao esquecimento, como consignado pela Comissão Europeia, tal unanimidade já não é atingida no segundo quadro a que se reporta PETER FLEISCHER e que contende com a eterna questão da cópia e republicação não autorizadas. Com efeito, na ótica dos padroeiros do direito ao esquecimento, tal conteúdo, em conformidade com o postulado na nova proposta, deverá ser, também ele, eliminado da plataforma em que se encontre, a menos que a manutenção da informação em causa seja necessária à luz da liberdade de expressão, como consta, aliás, da alínea a) do n.º 3 do artigo 17º, com remissão para o artigo 80º, que, por sua vez, salvaguarda a atividade jornalística, artística ou literária como exceção para a remoção de informação[259/260].

Esta ressalva, contudo, não inibe JEFFREY ROSEN de desmontar uma nova conjuntura que entende colocar em risco a integridade da liberdade de expressão. Para tal, recorre ao considerando 56 e ao n.º 1 do artigo 7º da nova proposta, onde está consagrada uma inversão do ónus da prova, em que é o próprio controlador de dados, neste caso o *website* responsável pelo processamento dos conteúdos, a demonstrar, perante uma autoridade de proteção de dados, que a publicação daquela informação foi realizada com o consentimento do seu titular, ou que a esta publicação subjaz um intuito jornalístico, artístico ou de cariz literário.

Para além disto, prevê a nova proposta que, se o titular original daquele conteúdo contactar a plataforma em questão para que remova a informação de quaisquer terceiros que dela se tenham apoderado, esta deverá tomar "todas as medidas razoáveis, incluindo medidas de caráter técnico"[261] para se assegurar que, também estes, procederam à sua remoção, uma

[258] Infelizmente, o exemplo de Max Schrems, acima analisado, mostra-nos uma realidade diferente.
[259] *Vide* arts 17º e 80º da nova proposta. Na verdade, já a Diretiva n.º 95/46/CE consagrava esta exceção para o tratamento de dados pessoais com fins exclusivamente jornalísticos, ou de expressão literária ou artística, no artigo 9º deste diploma.
[260] Também relacionada com a exceção consagrada no n.º 3 do artigo 17º da nova proposta, prende-se uma questão levantada por JERRY BRITO, e, de certa forma, já levantada por EUGENE VOLOKH, que encara esta exceção como uma espécie de livre arbítrio a ser exercido pelo Estado (através da sua autoridade nacional de proteção de dados que, de resto, se crê independente), ao decidir que tipo de informação se enquadra ao abrigo da liberdade de expressão e qual ficará fora do seu âmbito de proteção. Cfr. JERRY BRITO, *Your Right to Be Forgotten and My Right to Speak*, 07.06.2012. (Consult. 28.06.2012). Disponível em: http://jerrybrito.org/post/24629517011/your-right-to-be-forgotten-and-my-right-to-speak.
[261] *Vide* n.º 2 do artigo 17º da nova proposta.

vez que, se assim não proceder, incorrerá em pesadas sanções pecuniárias. Toda esta complexidade de procedimentos é alvo da inquietação de JEFFREY ROSEN, que teme que, desta forma, os controladores de dados pessoais optem por uma saída "mais fácil" de imediata eliminação do conteúdo em casos de resolução mais dúbia, o que, certamente, traria repercussões para a liberdade de expressão *online*[262].

Por último, surge-nos a terceira situação, apontada por PETER FLEISCHER, que analisa o direito de um individuo a ver apagada uma informação, verdadeira ou não, publicada sobre si, o que talvez levante as maiores preocupações quanto ao confronto presentemente em estudo. Nesta sede, JEFFREY ROSEN expõe nova fragilidade por parte da proposta, acusando-a, não só de proceder à remoção de informações verídicas, mas também de eliminar, sem diferenciação de procedimentos, qualquer informação que diga respeito ao indivíduo, independentemente de quem a tenha colocado *online,* seja uma informação verdadeira publicada por um órgão de comunicação social, seja uma fotografia publicada pelo próprio e que tenha, posteriormente, sido copiada por um terceiro[263].

O argumento de JEFFREY ROSEN prende-se, uma vez mais, com o exercício da inversão do ónus da prova, para quem a grande sequela de tal situação seria a eventual transformação de plataformas como o *Google Search* numa espécie de mecanismo de censura ao dispor da União Europeia, agindo em favor de um dos lados em disputa[264].

Todos estes considerandos levam a que, para alguns, o direito proposto pela Comissão Europeia seja não um direito a apagar a informação *detida* por si, mas um direito a apagar a informação *sobre* si[265].

Outro argumento, de resto curioso, apresentado prende-se, ainda, com o facto de o direito ao esquecimento não ser, na verdade, um direito relacionado com a privacidade. Este raciocínio que se afigura, à partida, paradoxal, apoia-se na ideia de que um direito relacionado com a privacidade deve ter, como objeto, informação que seja efetivamente privada. Contudo, para MIKE MASNICK, a forma de atuação do direito ao esquecimento, consiste, precisamente, em pegar em informação definida, por defeito, como pública (por estar disponível na Internet), e torná-la privada[266].

---

[262] Veja-se JEFFREY ROSEN, *The Right to Be Forgotten,* ob. cit., pp. 90 e 91.
[263] Cfr. JEFFREY ROSEN, *idem,* ob. cit., p. 91.
[264] Note-se que a *Google* não está ao abrigo da exceção prevista na proposta para o tratamento de informação pessoal com fins jornalísticos, artísticos ou literários.
[265] Veja-se JERRY BRITO, *Your Right to Be Forgotten and My Right to Speak*, ob. cit.
[266] Atente-se em MIKE MASNICK, Europeans *Continue To Push For 'Right To Be Forgotten'; Claim Americans 'Fetishize' Free Speech*, in Techdirt, 04.02.2011. (Consult. 28.06.2012). Disponível em:

Estas críticas não deixaram de ter resposta por parte da Comissão Europeia. Exercendo o seu direito ao contraditório, VIVIANE REDING já deixou claro que o direito ao esquecimento não foi concebido tendo como destinatário a atividade jornalística, referindo-se, em exclusivo, à recolha e utilização não autorizada de informação por parte das empresas[267].

Outros comentadores vieram, também, em auxílio da posição da Comissão, com o intuito de desmistificar as implicações da adoção deste direito na prática jornalística. JOHN HENDEL, num artigo explicitamente entitulado *Why Journalists Shouldn't Fear Europe's 'Right to Be Forgotten',* faz a apologia da exceção a que referimos *supra* quanto ao direito ao esquecimento não se aplicar à atividade da comunicação social, prevista, na nova proposta, à semelhança do que já acontecia na Diretiva que a precede[268/269].

No mesmo sentido, segue o discurso de DAVID LINDSAY, que denuncia o modo como a era digital cumulou de transparência as vidas de cada um, resultando, paradoxalmente, numa atitude cada vez mais impiedosa quanto às suas "indiscrições". Para este autor, as críticas à nova proposta da Comissão Europeia apenas poderão resultar de uma má interpretação da mesma, vendo a reforma como uma tentativa "modesta" da parte da União Europeia de restaurar algum equilíbrio a favor dos cibernautas para que possam, assim, obter um maior controlo sobre as suas informações pessoais[270].

Destarte, para DAVID LINDSAY, a proposta veio fazer frente à leviandade com que muitos dos utilizadores da *web* partilham a sua informação, colocando em evidência a

---

http://www.techdirt.com/articles/20110204/00145312961/europeans-continue-to-push-right-to-be-forgotten-claim-americans-fetishize-free-speech.shtml.

[267] Com efeito, a Comissão já se mostrou sensível aos diferentes cenários de recolha e processamento de dados pessoais *online*, tendo a Vice-Presidente da Comissão afiançado que "o direito ao esquecimento não é, com certeza, um direito absoluto", havendo situações em que há razões legítimas para que os dados pessoais dos utilizadores sejam mantidos. Num esforço para conquistar a confiança dos críticos face ao direito ao esquecimento, VIVIANE REDING não se coíbe, inclusivamente, de recorrer ao seu currículo político, relembrando já ter desempenhado o cargo de Comissária Europeia para os assuntos relacionados com os *media*, sendo que, como tal, não seria capaz de comprometer a integridade de direitos fundamentais como a liberdade de expressão e a liberdade de imprensa que tanto se dedicou a proteger. Cfr. VIVIANE REDING, *The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age,* (discurso para a Conferência da DLD), ob. cit.

[268] JOHN HENDEL, *Why Journalists Shouldn't Fear Europe's 'Right to Be Forgotten,* in The Atlantic, 25.01.2012. (Consult. 01.07.2012). Disponível em: http://www.theatlantic.com/technology/archive/2012/01/why-journalists-shouldnt-fear-europes-right-to-be-forgotten/251955/.

[269] JEFFREY ROSEN não deixa de fazer uma crítica a JOHN HENDEL, no seu artigo *The Right to Be Forgotten,* acusando HENDEL de alguma ingenuidade ao apenas fazer fé no discurso de VIVIANE REDING sem atentar ao texto da proposta que, ao definir amplamente dados pessoais como "qualquer informação que diga respeito ao indivíduo", não coloca na disponibilidade do direito ao esquecimento apenas as informações publicadas pelo próprio, mas também as informações publicadas sobre o próprio, o que colocaria em risco, contrariamente ao postulado por HENDEL, as liberdades de expressão e de imprensa. Cfr. JEFFREY ROSEN, *The Right to Be Forgotten,* ob. cit., p. 89.

[270] A este respeito, DAVID LINDSAY, *EU Privacy Laws: the 'Right to Be Forgotten' is Not Censorship*, ob. cit.

necessidade de atuação legal para garantir uma maior igualdade de interesses na relação entre utilizadores e fornecedores de serviços, no ciberespaço, sendo preferível proceder a este equilíbrio recorrendo a mecanismos legais, com o procedimento de reflexão que tal implica, do que deixar a questão à mercê de um política de autorregulação, que penderá, tendencialmente, para o lado do interesse economicista das empresas.

Salvaguardando a complexidade da conciliação entre o binómio privacidade e liberdade de expressão, o autor defende, contudo, que a manutenção da privacidade não significa uma oposição manifesta à liberdade de expressão, uma vez que se os indivíduos sentirem ter mais controlo sobre os seus dados pessoais, sentir-se-ão mais compelidos a partilhá-los. No mesmo sentido, também DANIEL SOLOVE, denuncia uma necessária promiscuidade entre privacidade e liberdade de expressão, no sentido em que a primeira tem um importante papel na efetivação da segunda, uma vez que a privacidade é necessária para proteger a autonomia pessoal dos indivíduos, bem como o diálogo político, necessário ao modelo democrático, e que, muitas vezes, se processa "à porta fechada"[271].

Por último, quanto às acusações de inoperabilidade prática do direito ao esquecimento, DAVID LINDSAY ressalva que a nova reforma não deverá ser entendida como um remédio absoluto, dadas as óbvias limitações inerentes à regulação do ciberespaço, pelo que a proposta se apresentará apenas como um importante contributo para devolver algum controlo aos utilizadores e impor consequências a algumas das práticas *online* que permanecem impunes e que, assim, continuam a incentivar um comportamento indecoroso por parte das empresas, a quem os clientes confiam as suas informações[272].

O debate entre os apologistas de um direito ao esquecimento e os seus detratores, apoiados no agravamento do conflito ideológico entre os EUA e a Europa que este direito representa, tenderá a não dar tréguas, pelo que talvez só a efetiva implementação da proposta possa esclarecer algumas dúvidas, afrouxando a discussão ou, quem sabe, acicatando-a. O que parece certo é que os paladinos da liberdade de expressão parecem decididos a não aceitar que as publicações na Internet se transformem em "mantas de retalhos" onde a informação seja substituída por avisos de eliminação da informação, restando apenas aos órgãos de comunicação social tradicionais a tarefa de documentar e imortalizar a História[273].

[271] Veja-se DANIEL J. SOLOVE, *The Future of Reputation…*, ob. cit., pp. 130 ss.
[272] Veja-se DAVID LINDSAY, *EU Privacy Laws: the 'Right to Be Forgotten' is Not Censorship,* ob. cit., *passim.*
[273] A este respeito, JOÃO PALMEIRO, *O Direito ao Esquecimento,* ob. cit., *passim.*

CONCLUSÕES

O direito ao esquecimento resulta, em primeira instância, da pretensão de atribuição aos indivíduos de um maior controlo sobre os dados pessoais que partilham nas inúmeras plataformas *online*, onde são alvo de um assédio hipnótico com funcionalidades inovadoras de comunicação, de entretenimento e de aquisição de bens e serviços. O direito ao esquecimento surge, assim, na sequência da tentativa de criação de um ambiente virtual seguro para os utilizadores, habilitando-os de um mecanismo que lhes permita remover as informações a seu respeito, quando não existam razões legítimas que suportem a sua subsistência e pelas quais foram inicialmente coletadas, ou tendo estes retirado o seu consentimento para a publicação[274].

Os dados pessoais fazem parte do património mais intrínseco ao indivíduo. Eles encerram todo o tipo de informações a seu respeito, umas mais delicadas do que outras - no caso dos dados pessoais sensíveis - mas todas essenciais à preservação da sua identidade e singularidade como cidadão, na medida em que se referem a informações que permitem a sua identificação. Face à sua preponderância, e ao estatuto de direito fundamental concedido à proteção de dados pessoais pela Constituição, mais concretamente, no artigo 35º, a sua derrogação apenas poderá ser realizada por motivos imperiosos, sempre submetidos ao crivo do princípio da proporcionalidade, de modo a garantir que a esfera da vida privada do cidadão apenas seja importunada na eventualidade de existir um interesse legítimo superior e somente na medida do estritamente necessário.

A recolha e tratamento de dados pessoais viu-se fortemente influenciada por um fenómeno de informatização que não só revolucionou os métodos de recolha destes dados, como potenciou a sua transmissão e interconexão, questão que gera ainda maiores preocupações quando falamos de fluxos de dados transfronteiras, especialmente quando se trate de um país de destino que não ofereça um "nível adequado de proteção".

Com efeito, nunca a protecção da privacidade se viu a braços com tamanhos desafios como na sociedade hodierna. A Internet veio revolucionar o modo como nos relacionamos e encurtar as barreiras físicas à comunicação entre os mais distantes quadrantes do planeta, estabelecendo-se como uma ferramenta da qual dificilmente poderemos abdicar, por mais comprometidos na nossa intimidade que, por vezes, nos sintamos.

[274] *Vide* artigo 17º e considerando 53 da nova proposta.

Por outro lado, a Internet trouxe consigo uma oportunidade de exercício da liberdade de expressão, até então limitada aos tradicionais meios de comunicação social, através dos inúmeros recursos colocados ao dispor dos seus utilizadores, a grande maioria de livre acesso. Aqui conquistaram, facilmente, destaque as redes sociais, *websites* vocacionados para a criação de perfis virtuais, personalizados pelos próprios utilizadores, que sustentam o seu apetite voraz por informação, resultando num autêntico ficheiro biográfico de cada um, quase sempre documentado com fotografia, vídeo e localização geográfica atualizada a cada ligação, assumindo-se como a verdadeira novidade nas formas de comunicação da última década. Estas plataformas, capitaneadas pelo *Facebook*, têm estado, nos últimos tempos, no centro de acesas polémicas envolvendo, precisamente, a forma como incentivam a partilha de informação pessoal perante os seus utilizadores, pelo modo, porventura, "demasiado zeloso" como a armazenam e, sobretudo, pela forma como procedem à sua comercialização para fins de publicidade personalizada, de que resulta a maioria dos seus proventos.

Analogamente se poderá referir o exemplo dos motores de busca, com um papel fundamental na difusão dos conteúdos, apresentando, ordenadamente, os resultados de uma pesquisa efetuada através da sua plataforma, ao vasculharem, quase instantaneamente, todo o universo publicamente acessível na *web*. Referência inegável neste mercado é a *Google*, cuja reputação tem sido abalada por controvérsias que tangem o modo como processa, armazena e utiliza, indevidamente e sem o seu consentimento, a informação dos seus utilizadores. De facto, a *Google*, assume-se como uma das empresas mais vanguardistas do espetro tecnológico, oferecendo já cerca de 60 serviços diferentes, que a sua nova política de privacidade se encarregou, unilateralmente, de centralizar numa única conta de utilizador, aumentando drasticamente as oportunidades de captação da informação sobre cada um.

Não obstante a polémica gerada em torno destes serviços, a verdade é que foi graças ao seu impulso que a economia digital não tardou a florescer, apoiada nas infinitas possibilidades de aplicação das plataformas virtuais, às quais qualquer um é bem-vindo, a troco de um registo nos *websites*, autênticas bases de operações das empresas que prosseguem a sua atividade através da Internet. É nesta partilha de dados pessoais que encontramos o motor desta economia virtual, obstinada em melhor conhecer o consumidor e, assim, lhe destinar, precisamente, os bens e serviços que assume serem adequados às sua pretensões. Aqui os dados pessoais dos utilizadores são uma verdadeira moeda de troca, um pouco à semelhança do ditado "informação é poder", ao possibilitar uma escrupulosa análise da

personalidade e dos comportamentos dos consumidores, permitindo, de certa forma, "viciar" as leis da oferta e da procura, brindando o consumidor, precisamente, com aquilo que deseja.

Percebem-se, assim, as preocupações vocalizadas pelas grandes empresas e grupos económicos, relacionadas com a atribuição de um maior controlo sobre os dados pessoais aos utilizadores/consumidores de bens e serviços *online*.

Estas preocupações agudizaram-se aquando do anúncio, por parte da Comissão Europeia, da adoção de uma nova reforma no âmbito da proteção de dados pessoais, tendo no horizonte o contexto da *World Wide Web*, algo que a Diretiva n.º 95/46/CE não foi capaz de antever. Prosseguindo com os esforços de agilização desta economia digital, e colocando a tónica na implementação de um direito ao esquecimento, foi propósito da Comissão reforçar o funcionamento do mercado único da UE e aumentar a sua competitividade - assumindo-se o mercado único europeu como uma espécie de *gold standard* dos mercados mundiais[275] - sem negligenciar, em tempo algum, os baluartes em que assentou a sua edificação, como a garantia das liberdades de circulação de bens, serviços, pessoas e capitais, e a harmonização dos quadros legislativos de cada Estado-membro. Esta harmonização pretende ser conseguida através da uniformização das várias leis de proteção de dados pessoais num único instrumento jurídico, aplicável aos 27 Estados-membros, permitindo que qualquer conflito neste âmbito, decorrido em território comunitário, ou envolvendo agentes estrangeiros aqui sediados, seja resolvido com recurso a um único enquadramento disponível e envolvendo uma única autoridade de proteção de dados, o que pressupõe uma ágil cooperação entre todos estes organismos.

É objetivo da Comissão que a certeza jurídica, assim proporcionada, se traduza nas condições ideais ao investimento e consequente desenvolvimento da economia europeia e dos agentes que nela efetuem as suas transações, ao mesmo tempo que se procede a uma simplificação nos procedimentos burocráticos.

Vemos, inclusive, que a confiança por parte dos intervenientes, sobretudo por parte dos consumidores, tem aqui um papel da mais extrema relevância, uma vez que, para que estes confiem os seus dados pessoais, fonte energética desta economia digital, é necessário que sejam criados expedientes que lhes assegurem que as suas informações sejam armazenadas dignamente, com o seu consentimento, e para os fins para que foram recolhidas

[275] Neste sentido, VIVIANE REDING, *Towards a New 'Gold Standard' in Data Protection,* 19.03.2012. (Consult. 01.07.2012). Disponível em: http://ec.europa.eu/commission_2010-2014/reding/pdf/speeches/20120319speech-data-gold-standard_en.pdf.

inicialmente, abstendo-se os controladores de proceder a utilizações abusivas com efeitos perversos para a privacidade do seu titular. Pretende-se, assim, contrariar o grande entrave a que o comércio eletrónico se estabeleça como dominante face aos modelos de comércio tradicional, promovendo uma relação de benefício mútuo entre empresas e consumidores.

Contudo, por muito bem-intencionada que, na teoria, aparente ser a nova proposta da Comissão, a verdade é que grandes empresas como a *Google*, desde logo, manifestaram a sua oposição, com orientações antagónicas quanto a quem deverá caber a responsabilidade de eliminar os conteúdos que os utilizadores considerem ferir a sua intimidade e, até, que tal eliminação deva ser, tão-pouco, realizada.

Esta problemática remete-nos para o manifesto conflito ideológico entre as duas margens do Atlântico, conflito esse que a nova proposta se encarregou de adensar. Com efeito, atentamos que, nos EUA, uma jurisprudência legitimada pela Primeira Emenda à Constituição teima em não reconhecer um direito à autodeterminação informativa aos seus cidadãos e, no mesmo sentido, parece pouco permeável à ideia da introdução de um direito que permita aos utilizadores de plataformas *online* remover a informação que já não pretendem ver publicada, derrubando qualquer obstáculo que pareça atravessar-se à frente do seu semiendeusado direito à liberdade de expressão.

Por seu lado, é na Europa que se verifica uma maior intervenção a respeito da proteção das informações pessoais dos cidadãos, fenómeno a que não é alheia, como vimos, a própria intervenção da UE. A disparidade de posições entre Europa e EUA está, também, evidenciada no confronto aceso entre os detratores do direito ao esquecimento, motivados pelas efeitos perversos que este poderá acarretar para as liberdades de expressão e de imprensa, e aqueles que, pelo contrário, apoiam a sua implementação. Temem os críticos que este expediente instale um clima de propensão para a remoção desenfreada de conteúdos, uma vez que a Comissão Europeia planeia impor, sobre os controladores de dados, a obrigação de eliminar as publicações que digam respeito a determinado indivíduo que as queira ver removidas, urgindo a que os controladores procedam a essa remoção, ou comprovem que tal conteúdo se encontra publicado ao abrigo da exceção consagrada na alínea a) do n.º 3 do artigo 17º da nova proposta e que se refere à publicação de conteúdos com intuito jornalístico, artístico ou literário.

Incontornáveis são, igualmente, as situações em que se verifique cópia ou republicação dessa informação por terceiros, aqui impondo a nova proposta que o controlador

aja no sentido de satisfazer os interesses do titular das informações, instando, de forma tão eficaz quanto possível, a que o terceiro remova a publicação, na certeza, porém, de que, sobre o controlador, impenderá, a todo o momento, o ónus da prova, que o incumbe de demonstrar que tomou "todas as medidas razoáveis, incluindo medidas de caráter técnico"[276], para concluir aquela pretensão. As sanções que, de outra forma, se imporão aos controladores, temem os críticos, que sirvam como meio de coação a que os controladores de dados facilitem na eliminação dessa informação, o que, estando em causa grandes plataformas virtuais como o *Google Search*, colocaria em marcha um imediato clima de censura orquestrado pelos governos ao estilo orwelliano dos *memory holes* para eliminar factos inconvenientes.

Perante todas as acusações, a Comissão não se coibiu de esclarecer, contudo, que o direito ao esquecimento se destina, unicamente, às empresas que fazem uso dos dados pessoais dos seus clientes/utilizadores. Para VIVIANE REDING, este direito tem, assim, como propósito único, equilibrar a relação entre os cibernautas e as empresas que recolhem e fazem uso dos seus dados pessoais, colocando-os numa maior posição de controlo quanto ao seu destino.

Ora, tanto o comércio eletrónico, como as redes sociais e, ainda, uma imprensa digital em permanente atualização, coadjuvados por motores de busca que, em décimos de segundo, agregam toda a informação, colocam o direito à autodeterminação informativa numa posição de singular fragilidade. Tal dificulta ao indivíduo o controlo da informação que sobre si circula, bem como, a preservação dos seus dados pessoais, em prejuízo da sua reserva da intimidade da vida privada.

O direito à reserva da intimidade da vida privada surge, na nossa discussão, como o derradeiro direito fundamental a salvaguardar que, assim, se serve das normas conferidas à proteção de dados pessoais para defletir os ataques à sua integridade. É neste sentido que a implementação de um direito ao esquecimento poderá revelar-se um valioso acrescento ao enquadramento legislativo europeu nesta matéria[277], na certeza, porém, de que enfrentará titânicos obstáculos à sua aplicação, pelo que não deverá, apesar de tudo, a nova proposta ser encarada como um remédio absoluto para o problema da proteção de dados pessoais.

Assim, cremos que também o auxílio técnico, por parte da mesma tecnologia que dificulta a implementação do direito ao esquecimento, poderá ser aqui uma solução

[276] *Vide* n.º 2 do artigo 17º da nova proposta.

[277] Neste sentido, afirma JEF AUSLOOS, *The 'Right to Be Forgotten'…,* ob. cit., p. 17, *[a]n adequate implementation of the 'right to be forgotten' will definitely contribute to a shift in the power balance, to the benefit of each and every individual in the information society.*

aproximada, através da inclusão de sistemas de "privacidade por defeito" aquando da construção dos interfaces das plataformas *online,* para que o utilizador continue a usufruir das potencialidades desta era digital, sem que, para isso, tenha de pagar a pesada fatura de ver a sua privacidade comprometida.

Nas palavras de GARCIA MARQUES e LOURENÇO MARTINS, "[n]as sociedades de hoje, é necessário, na medida do possível, encontrar formas de defesa contra a complexificação crescente das relações sociais, preservando nichos de intimidade, de resguardo e de reserva – em suma, refúgios de individualidade. Se é certo, por um lado, que aos fenómenos da solidão e da exclusão há que opor manifestações de solidariedade e de inserção sociais, também, como contraponto, para resistir à febre e ao stress da vida em multidão, é imperioso contrapor ambientes de isolamento e de à vontade, tomando-se consciência de que a intimidade da vida privada e familiar é o único circulo onde a pessoa pode ser o que realmente é. E, como último reduto da intimidade pessoal, tem que ser protegido"[278].

[278] GARCIA MARQUES, LOURENÇO MARTINS, *Direito da Informática…,* ob. cit., p. 442.

BIBLIOGRAFIA

MONOGRAFIAS:

- ASCENSÃO, JOSÉ DE OLIVEIRA, *Direito Civil: Teoria Geral, Vol. I: Introdução, as Pessoas, os Bens*, Coimbra, Coimbra Editora, 1997;
- ASCENSÃO, JOSÉ DE OLIVEIRA, *Estudos sobre Direito da Internet e da Sociedade de Informação*, Coimbra, Almedina, 2001;
- AUSLOOS, JEF, *The 'Right to Be Forgotten' – Worth Remembering?*, in Computer Law and Security Review 2012, 09.12.2011.
  Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1970392 ;
- BELLEIL, ARNAUD, *@ Privacidade: o Mercado dos Dados Pessoais; Proteção da Vida Privada na Idade da Internet*, Instituto Piaget, 2002;
- BLANDIN-OBERNESSER, ANNIE, *L'Union Européenne et Internet*, Rennes, Editions Apogée, 2001;
- BRIN, DAVID, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?*, Nova Iorque, Basic Books, 1999;
- CAMPUZANO, HERMINIA TOMÉ, *Vida Privada y Datos Personales: Su Protección Jurídica Frente a la Sociedad de la Información*, Madrid, Editorial Tecnos, 2000;
- CANOTILHO, J. J. GOMES; MOREIRA, VITAL, *Constituição da República Portuguesa Anotada, Vol. I*, 4ª Ed., Coimbra, Coimbra Editora, 2007;
- CASSANO, GIUSEPPE, *Dirito Dell'Internet, Il Sistema di Tutele della Persona, Milão,* Giuffrè Editore, 2005;
- CASTRO, CATARINA SARMENTO E, *Direito da Informática, Privacidade e Dados Pessoais*, Coimbra, Almedina, 2005;
- FACHANA, JOÃO, *A Responsabilidade Civil pelos Conteúdos Ilícitos Colocados e Difundidos na Internet,* Dissertação de Mestrado em Direito (Área de Especialização em Ciências Jurídico Privatísticas), Porto, Faculdade de Direito da Universidade do Porto, julho 2011.
- FARINHO, DOMINGOS SOARES, *Intimidade da Vida Privada e Media no Ciberespaço*, Coimbra, Almedina, 2007;
- FEILER, LUKAS, Information *Security Law in the EU and the U.S. – A Risk-Based Assessment of Regulatory Policies,* Viena e Nova Iorque, Springer, 2011;
- FERNANDES, HÉLÈNE MARINE SERRA, *O Direito Penal do Inimigo: Reconfiguração do Estado de Direito?* Dissertação de Mestrado em Direito (Área de Especialização em Ciências Jurídico Políticas), Porto, Faculdade de Direito da Universidade do Porto, julho 2011.
- GONÇALVES, MARIA EDUARDA, *Direito da Informação: Novos Direitos e Formas de Regulação na Sociedade de Informação*, Coimbra, Almedina, 2003;
- MAIA, FERNANDO JOAQUIM FERREIRA, *O Habeas Data Brasileiro na Perspetiva da sua Inefetividade e como Instrumento do Acesso à Justiça*. Disponível em: http://www.conpedi.org.br/manaus/arquivos/anais/recife/efetividade_fernando_joaquim_maia.pdf ;
- MARQUES, GARCIA; MARTINS, LOURENÇO, *Direito da Informática*, Coimbra, Almedina, 2006;
- MAYER-SCHÖNBERGER, VIKTOR, *Delete: The Virtue of Forgetting in the Digital Age*, Princeton e Oxford, Princeton University Press, 2009;
- PEREIRA, JOEL TIMÓTEO RAMOS, *Direito da Internet e Comércio Electrónico*, Lisboa, Quid Juris Sociedade Editora, 2001;
- PINTO, PAULO DA MOTA, *A Limitação Voluntária do Direito à Reserva sobre a Intimidade da Vida Privada*, in *Estudos em Homenagem a Cunha Rodrigues, Vol. II*, Coimbra, Coimbra Editora, 2002;

- QUEIROZ, CRISTINA, *A Proteção Constitucional da Recolha e Tratamento de Dados Pessoais Automatizados*, in *Homenagem da Faculdade de Direito de Lisboa ao Professor Doutor Inocêncio Galvão Telles, 90 Anos*, Coimbra, Almedina, 2007;
- ROSEN, JEFFREY, *The Right to Be Forgotten*, Stanford Law Review Online, 64, 13.02.2012;
- SMITH, GRAHAM J. H. *et al.*, *Internet Law and Regulation*, 2ª Ed., Londres. FT Law and Tax, 1997;
- SOLOVE, DANIEL J., *The Digital Person: Technology and Privacy in the Information Age*, Nova Iorque e Londres, New York University Press, 2004;
- SOLOVE, DANIEL J., *The Future of Reputation: Gossip, Rumor and Privacy on the Internet*, New Haven e Londres, Yale University Press, 2007;
- VOLOKH, EUGENE, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000). Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=200469 ;
- WALDEN, IAN, *Data Protection* in *Computer Law*, in CHRIS REED, JOHN ANGEL (coord.), *Computer Law*, 4ª Ed., Londres, Blackstone Press Limited, 2000;
- WARREN, SAMUEL, BRANDEIS, LOUIS, *The Right to Privacy*, in Harvard Law Review, V. IV, n.º 5, 1890 ;
- WEBER, ROLF H., *The Right to Be Forgotten: More Than a Pandora's Box?*, in JIPITEC, Vol. 2, 2011, p. 120. Disponível em: http://www.jipitec.eu/issues/jipitec-2-2-2011/3084 ;
- WERRO, FRANZ, *The Right to Inform v. the Right to be Forgotten: a Transatlantic Clash*, in Center for Transnational Legal Studies Colloquium, Georgetown University, 05.2009. Disponível em: http://ssrn.com/abstract=1401357 ;
- WHITMAN, J. Q., *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 Yale L. J., 2004;
- ZITTRAIN, JONATHAN L., *The Future of the Internet and How to Stop It*, New Haven e Londres, Yale University Press, 2008.

SITIOS DA INTERNET:

- BARTZ, DIANE, *Obama Administration Seeks Internet Privacy Bill*, in Reuters, 17.03.2011. (Consult. 04.05.2012). Disponível em: http://www.reuters.com/article/2011/03/17/us-privacy-obama-idUSTRE72F83U20110317 ;
- BRIGHT, PETER, *Europe Proposes a Right to Be Forgotten*, in Ars Technica, 26.01.2012. (Consult. 20.06.2012). Disponível em: http://arstechnica.com/tech-policy/2012/01/eu-proposes-a-right-to-be-forgotten/ ;
- BRITO, JERRY, *Your Right to Be Forgotten and My Right to Speak*, 07.06.2012. (Consult. 28.06.2012). Disponível em: http://jerrybrito.org/post/24629517011/your-right-to-be-forgotten-and-my-right-to-speak ;
- COMISSÃO EUROPEIA, *Why Do We Need an EU Data Protection Reform?* (Consult. 25.05.2012). Disponível em: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf ;
- COMISSÃO EUROPEIA, *How Will the Data Protection Reform Affect Social Networks?* (Consult. 25.05.2012). Disponível em: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf ;
- COMISSÃO EUROPEIA, *How Will the EU's Reform Adapt Data Protection Rules to New Technological Developments?*, p. 1. (Consult. 25.11.11). Disponível em: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/8_en.pdf ;

- COMISSÃO EUROPEIA, *Think Before You Post!*, 09.02.10. (Consult. 05.04.12). Disponível em: http://ec.europa.eu/news/science/100209_1_en.htm ;
- COMISSÃO EUROPEIA, *Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses – press release*, 25.01.2012. (Consult. 22.02.12). Disponível em: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46 ;
- COMISSÃO EUROPEIA, *How Will the EU's Data Protection Reform Strengthen the Internal Market*, p. 1. (Consult. 19.06.2012). Disponível em: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/4_en.pdf ;
- COMISSÃO EUROPEIA, *How Will the EU's Data Protection Reform Benefit European Businesses?* (Consult. 25.06.2012). Disponível em: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/7_en.pdf ;
- COMISSÃO EUROPEIA, *New Rules: New Benefits for Business*. (Consult. 23.06.2012). Disponível em: http://ec.europa.eu/justice/data-protection/minisite/business4.html ;
- COMISSÃO EUROPEIA, *European Commission Sets Out Strategy to Strengthen EU Data Protection Rules*, 04.11.2010. (Consult. 28.06.2012). Disponível em: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1462 ;
- CROVITZ, L. GORDON, *Forget Any 'Right to Be Forgotten'*, in The Wall Street Journal, 15.11.2010. (Consult. 23.06.2012). Disponível em: http://online.wsj.com/article/SB10001424052748704658204575610771677242174.html ;
- DALEY, SUZANNE, *On Its Own, Europe Backs Web Privacy Fights*, in The New York Times, 09.08.2011. (Consult. 15.03.2012). Disponível em: http://www.nytimes.com/2011/08/10/world/europe/10spain.html?_r=2&%20sq=european%20privacy&st=cse&scp=1&pagewanted=all ;
- DIEHN, SONYA ANGELICA, *Spanish Firm Loses 'Right to Be Forgotten'*, in Deutsche Welle, 28.02.2012. (Consult. 23.06.2012). Disponível em: http://www.dw.de/dw/article/0,,15774283,00.html ;
- DOU, EVA, *Internet Privacy and the 'Right to Be Forgotten'*, in Reuters, 17.03.2011. (Consult. 14.03.2012). Disponível em: http://www.reuters.com/article/2011/03/17/us-eu-internet-privacy-idUSTRE72G48Z20110317 ;
- FLEISCHER, PETER, *Our Thoughts on the Right to Be Forgotten*, in *Google* European Public Privacy Blog, 12.02.2012. (Consult. 16.05.2012). Disponível em: http://googlepolicyeurope.blogspot.pt/2012/02/our-thoughts-on-right-to-be-forgotten.html ;
- FLEISCHER, PETER, *Foggy Thinking About the Right to Oblivion*, 09.03.2011. (Consult. 22.06.2012). Disponível em: http://peterfleischer.blogspot.pt/2011/03/foggy-thinking-about-right-to-oblivion.html ;
- HENDEL, JOHN, *Why Journalists Shouldn't Fear Europe's 'Right to Be Forgotten,* in The Atlantic, 25.01.2012. (Consult. 01.07.2012). Disponível em: http://www.theatlantic.com/technology/archive/2012/01/why-journalists-shouldnt-fear-europes-right-to-be-forgotten/251955/ ;
- HUNTON & WILLIAMS LLP, *French Government Secures "Right to Be Forgotten" on the Internet*, 21.10.2010. (Consult. 06.04.2012). Disponível em: http://www.huntonprivacyblog.com/2010/10/articles/french-government-secures-right-to-be-forgotten-on-the-internet/ ;

- LAWSON, KENT, *Do We Need a Right to Be Forgotten on the Internet?* in Private Wifi, 19.09.2011. (Consult. 12.12.2011). Disponível em: http://www.privatewifi.com/do-we-need-a-right-to-be-forgotten-on-the-internet/ ;
- LAWSON, KENT, *Online Reputation: What the Search Giants Know About You, Part 1*, 20.06.2011. (Consult. 18.03.2012). Disponível em: http://www.privatewifi.com/online-reputation-what-the-search-giants-know-about-you-part-1/ ;
- LINDSAY, DAVID, *EU Privacy Laws: The 'Right to Be Forgotten' is Not Censorship*, in Crikey, 21.02.2012. (Consult. 06.06.2012). Disponível em: http://www.crikey.com.au/2012/02/21/eu-privacy-laws-the-right-to-be-forgotten-is-not-censorship/ ;
- LOCKE, LAURA, *Facebook Ireland Accused of Creating 'Shadow Profiles' on Users, Nonusers*, in Cnet News, 21.10.2011. (Consult. 15.06.2012). Disponível em: http://news.cnet.com/8301-1023_3-20123919-93/facebook-ireland-accused-of-creating-shadow-profiles-on-users-nonusers/?part=rss&subj=news&tag=2547-1_3-0-20 ;
- MARTINS, ALEXANDRE, *Empresas dos Estados Unidos Pedem Password do Facebook aos Candidatos a Emprego*, in Público, 26.03.2012. (Consult. 14.06.2012). Disponível em: http://www.publico.pt/Mundo/empresas-norteamericanas-pedem-dados-de-acesso-ao-facebook-aos-candidatos-a-emprego-1539453 ;
- MASNICK, MIKE, *Europeans Continue To Push For 'Right To Be Forgotten'; Claim Americans 'Fetishize' Free Speech*, in Techdirt, 04.02.2011. (Consult. 28.06.2012). Disponível em: http://www.techdirt.com/articles/20110204/00145312961/europeans-continue-to-push-right-to-be-forgotten-claim-americans-fetishize-free-speech.shtml ;
- MEYER, DAVID, *EU Puts Google Straight on 'Right to Be Forgotten'*, in ZDNet UK, 22.02.2012. (Consult. 20.06.2012).
  Disponível em: http://www.zdnet.co.uk/news/security/2012/02/22/eu-puts-google-straight-on-right-to-be-forgotten-40095097/ ;
- MEYER, DAVID, *EU Justice Chief: Google is Playing Privacy Games*, in ZDNet UK, 02.03.2012. (Consult. 22.06.2012).
  Disponível em: http://www.zdnet.co.uk/blogs/communication-breakdown-10000030/eu-justice-chief-google-is-playing-privacy-games-10025538/ ;
- PEIXOTO, MARCO AURÉLIO VENTURA, *Habeas Data: A Polêmica Garantia Constitucional de Conhecimento e Retificação de Informações Pessoais em Poder do Estado*, in Jus Navigandi, Teresina, ano 6, n. 52, 01.11.2001. (consult. 10.01.2012). Disponível em: http://jus.com.br/revista/texto/2362 ;
- PRUMMER, JULIA, *Max Schrems Não 'Gosta' do Facebook*, in Presseurop, 27.04.2012. (Consult. 14.06.12). Disponível em: http://www.presseurop.eu/pt/content/article/1881381-max-schrems-nao-gosta-do-facebook ;
- PALMEIRO, JOÃO, *O Direito ao Esquecimento*, in Setúbal na Rede, 23.05.2011. (Consult. 23.06.2012).
  Disponível em:
  http://www.setubalnarede.pt/content/index.php?action=articlesDetailFo&rec=14802 ;
- REDING, VIVIANE, *The EU Data Protection Reform 2012: Safeguarding Privacy in a Connected World*, (discurso de apresentação da nova reforma), Bruxelas, 25.01.2012. (Consult. 20.05.2012). Disponível em:
  http://ec.europa.eu/commission_2010-2014/reding/pdf/speeches/data-protection-reform2012_en.pdf ;
- REDING, VIVIANE, *Towards a New 'Gold Standard' in Data Protection,* 19.03.2012. (Consult. 01.07.2012). Disponível em:

http://ec.europa.eu/commission_2010-2014/reding/pdf/speeches/20120319speech-data-gold-standard_en.pdf ;

- REDING, VIVIANE, *The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age*, (discurso para a Conferência da DLD), Munique, 22.01.2012. (Consult. 20.05.2012).
  Disponível em: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26 ;
- ROBERTSON, STRUAN, *Hasty Legislation Will Make a Mess of Europe's 'Right to Be Forgotten'*, in Out-Law, 12.11.2010. (Consult. 03.05.2012). Disponível em: http://www.out-law.com/page-11544 ;
- SCHWARTZ, JOHN, *Two German Killers Demanding Anonymity Sue Wikipedia's Parent*, in The New York Times, 12.11.2009. (Consult. 23.06.2012).
  Disponível em: http://www.nytimes.com/2009/11/13/us/13wiki.html ;
- SHEARMAN, SARAH, *Facebook Settles With FTC Over Privacy Complaints*, in BrandRepublic, 30.11.2011. (Consult. 16.16.2012).
  Disponível em: http://www.brandrepublic.com/news/1106970/Facebook-settles-FTC-privacy-complaints/ ;
- SIRY, LAWRENCE, SCHMITZ, SANDRA, *Online Archives on Trial In Germany: Is there a Right to Be Forgotten?*, 2011, (Consult. 23.06.2012) Disponível em: http://www.law.mmu.ac.uk/wp-content/uploads/2011/04/Online-Archives-on-Trial-in-Germany.pdf ;
- TARRAN, BRIAN, *'Right to Be Forgotten' is Unenforceable, says ICO*, in Research-Live, 17.11.2011. (Consult. 03.05.2012). Disponível em: http://www.research-live.com/news/government/right-to-be-forgotten-is-unenforceable-says-ico/4006419.article ;
- TARRAN, BRIAN, *The 'Right to be Forgotten' is a 'False Expectation'*, in Research-Live. (Consult. 03.05.2012). Disponível em: http://www.research-live.com/the-right-to-be-forgotten-is-a-false-expectation/4006392.blog ;
- WARMAN, MATT, *Online 'Right to Be Forgotten' confirmed by EU*, in The Telegraph, 17.03.11. (Consult. 03.04.12).
  Disponível em: http://www.telegraph.co.uk/technology/internet/8388033/Online-right-to-be-forgotten-confirmed-by-EU.html ;
- WARMAN, MATT, *EU Fights 'Fierce Lobbying' to Devise Data Privacy Law*, in The Telegraph, 09.02.2012. (Consult. 14.03.2012).
  Disponível em: http://www.telegraph.co.uk/technology/internet/9069933/EU-fights-fierce-lobbying-to-devise-data-privacy-law.html .

JURISPRUDÊNCIA

- Ac. do Supremo Tribunal Administrativo de 19 de junho de 1997, Proc. n.º 042310. Disponível em: http://www.dgsi.pt/ ;
- Ac. do Tribunal de Justiça das Comunidades Europeias de 6 de novembro do 2003. N.º C-101/01. Disponível em:
  http://curia.europa.eu/juris/showPdf.jsf;jsessionid=9ea7d0f130d5cb7adb49e2fe4fe5af4cda4178d90ead.e34KaxiLc3eQc40LaxqMbN4Oa3aNe0?text=&docid=48382&pageIndex=0&doclang=PT&mode=doc&dir=&occ=first&part=1&cid=1218293.