

# DIREITOS FUNDAMENTAIS E TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO

JORGE PEGADO LIZ

Advogado. Membro do CESE (Bruxelas)

## EXCERTOS

*“De um modo sucinto, poderemos afirmar que as principais características das RSC consistem na tendencial gratuidade do serviço, o rápido e exponencial crescimento do número de utilizadores, a sua extraordinária valorização económica, a facilidade de utilização e a disponibilização de funcionalidades que permitem a interação entre os utilizadores dos serviços”*

*“Existe um ‘fosso entre gerações’, potencialmente cada vez maior, entre, por um lado, a utilização das tecnologias em linha e a percepção dos seus riscos pelas crianças e jovens, e, por outro lado, a compreensão destes modos de utilização pelos adultos”*

*“A proteção do utilizador, em particular do utilizador vulnerável, especialmente das crianças, mas também o caso de outros públicos mais sensíveis ou vulneráveis, como os idosos, os diminuídos físicos ou psíquicos, é uma prioridade que não deve ser assumida unicamente pelas pessoas encarregadas da sua guarda e educação”*

*“A criação de um ‘fórum da juventude’ poderia ser útil para a participação dos jovens e para a difusão de informações junto das redes sociais utilizadas pelos grupos mais vulneráveis”*

*“O direito à proteção de dados pessoais não é absoluto, mas deve ser considerado em relação à sua função na sociedade”*

## 1. Novos instrumentos e novas tecnologias de informação, de comunicação e de entretenimento

1.1. A internet e as tecnologias das comunicações (a seguir designadas por “tecnologias em linha”) foram previstas e concebidas como instrumentos de comunicação para os representantes do mundo académico e os investigadores; contudo, atualmente são utilizadas em privado, nas empresas e nas administrações públicas na maior parte dos países do mundo.

1.2. As Redes Sociais de Comunicação (RSC) caracterizam-se, no essencial, por serem serviços em linha que têm por finalidade a criação e agregação de comunidades de pessoas que partilham atividades ou interesses comuns, ou que estejam simplesmente interessadas em conhecer as preferências e as atividades de outras pessoas, e que disponibilizam um conjunto de funcionalidades que permitem a interação entre os utilizadores<sup>1</sup>.

1.3. As RSC apresentam uma rápida expansão (alegadamente 211 milhões de pessoas e aproximadamente três quartos dos internautas, estimados em 282,7 milhões, frequentam regularmente estes serviços *online*), sendo fundamentalmente utilizados por jovens a partir dos 16 anos, mas com uma taxa de fidelidade relativamente reduzida no caso de alguns serviços. Em 2009 a Comissão<sup>2</sup> estimava que as RSC atraíam cerca de 40 milhões de utilizadores regulares na Europa, logo no ano seguinte a sua utilização aumentou cerca de 35% e as estimativas para 2011 aproximam-se dos 200 milhões sendo responsável por cerca de quatro minutos de cada cem passados *online*, e representa mais de 30% do tempo total passado em *sites* de RSC.

1.4. Paralelamente, as marcas multinacionais aderiram ao novo fenómeno publicitando cada vez mais os seus produtos e serviços nas RSC, por vezes de forma desleal. A partir da campanha de Obama, também as máquinas partidárias resolveram utilizar estes novos serviços, como se verificou nas recentes eleições para o Parlamento Europeu. O próprio Vaticano aderiu ao Facebook (Pope2you.net). Até o nosso PR “twitta”.

## 2. A noção de “meio virtual”: vantagens e perigos; a importância de saber fazer

2.1. De um modo sucinto, poderemos afirmar que as principais características das RSC consistem na tendencial gratuidade do serviço, o rápido e exponencial crescimento do número de utilizadores, a sua

extraordinária valorização económica, a facilidade de utilização e a disponibilização de funcionalidades que permitem a interação entre os utilizadores dos serviços.

Os serviços de RSC na internet são um fenómeno social emergente, cuja componente tecnológica se acha em permanente evolução e que reconhecidamente altera o modo como as pessoas se inter-relacionam e interagem umas com as outras através da internet.

**2.2.** A internet melhorou a qualidade de vida de muitas pessoas, especialmente dos jovens, dos idosos e de pessoas com deficiências. Constitui um instrumento de comunicação único, que atualmente se torna cada vez mais uma “rede social”. A emergência de novas tecnologias e serviços é fundamental para a inovação e o crescimento das empresas do mundo inteiro. Os jovens são frequentemente os primeiros a compreender as possibilidades destas inovações e a adoptá-las. Todavia, esta evolução é acompanhada de abusos, o que constitui uma preocupação cada vez maior.

A nova dinâmica dos estilos de vida, das famílias e dos modelos de emprego provocou mais períodos de independência ou isolamento. São incontestáveis os aspectos positivos associados ao desenvolvimento das RSC, designadamente, o seu contributo para:

- (i) a garantia e o exercício da liberdade de expressão em determinados contextos sociais e políticos;
- (ii) a criação e agregação de comunidades em linha;
- (iii) o (re)encontro de amigos e familiares e a possibilidade de comunicarem entre si;
- (iv) a prevenção de situações de risco para os menores e a possibilidade destes pedirem ajuda através das RSC;
- (v) a promoção de bens e de serviços e o incremento do comércio electrónico.

**2.3.** Importa, no entanto, ter em atenção que principalmente as crianças utilizam de maneira ativa, e cada vez mais, as tecnologias em linha. Não obstante as vantagens da interatividade e da participação no ambiente em linha, as crianças também estão confrontadas com consideráveis riscos associados à utilização das RSC para fins ilícitos ou prejudiciais, designadamente ao desenvolvimento dos menores<sup>3</sup>, de que se destacam, entre outros:

- a) prejuízo direto enquanto vítimas de exploração sexual documentada por fotografias, filmes ou ficheiros de áudio divulgados em linha (material pedopornográfico);

b) perpetuação da exploração sexual das vítimas através do confronto visual repetido com os registos que são amplamente divulgados em linha e estão disponíveis em todo o mundo;

c) contato direto com os predadores que procuram estabelecer relações de amizade com o objetivo de cometerem abusos sexuais (aliciamento);

d) vítimas de assédio no ambiente em linha (ciberassédio);

e) a verificação de traumas psicológicos originados por insultos veiculados por meio desses serviços;

f) a exibição de fotografias e de vídeos com adolescentes nus ou seminus, próprios ou de outros;

g) os anúncios explícitos de prostituição e de serviços de “acompanhamento” (escort);

h) a violação reiterada da privacidade e da honra e dignidade pessoal;

i) o atentado à saúde física e mental dos seus utilizadores;

j) os apelos à violência, ao racismo e à xenofobia;

k) a divulgação de ideologias totalitárias de carácter fascista ou fazendo a apologia do nazismo;

l) os suicídios de jovens, alegadamente em consequência da divulgação de certas situações do foro íntimo através destas redes.

Acresce que existe um “fosso entre gerações”, potencialmente cada vez maior, entre, por um lado, a utilização das tecnologias em linha e a percepção dos seus riscos pelas crianças e jovens, e, por outro lado, a compreensão destes modos de utilização pelos adultos.

**2.4.** Deverá igualmente ser tido em consideração a nova geração de tecnologias associadas às RSC, designadamente as aplicações que permitem a geolocalização dos utilizadores de tais redes, as que recorrem a tecnologias de reconhecimento de rostos permitindo a sua associação a contas de RSC e as novas possibilidades de interação com os telefones móveis da última geração.

Acresce a circunstância deste tipo de redes serem facilmente utilizadas para a disseminação de vírus, como aquele que afetou o *Twitter* no fim de semana de 11 e 12 de abril de 2009 e gerou automaticamente mais de 100.000 mensagens, prejudicando um número indeterminado de contas.

**2.5.** No âmbito da iniciativa *Safer Internet Forum*, a Comissão submeteu a consulta pública<sup>4</sup> um questionário que abordou a temática das RSC, podendo

Os serviços de  
RSC na internet  
são um  
fenômeno social  
emergente

extrair-se da leitura dos contributos recebidos<sup>5</sup> que o *cyberbullying*, a invasão da privacidade e o *grooming* foram apontados como os principais e mais comuns perigos que os menores enfrentam na utilização das RSC.

**2.5.1.** A propósito do *cyberbullying*<sup>6</sup>, constata-se que 54% dos pais europeus estão preocupados com a possibilidade dos seus filhos poderem ser vítimas de tal prática. Mais de 80% dos pais na França, Grécia e Portugal estão preocupados com a possibilidade dos seus filhos serem objeto de *bullying* quando utilizem a internet ou o telemóvel. Já em certos países com forte tradição na defesa dos direitos das crianças e na sua educação, como na Dinamarca, na Suécia e na Finlândia, os pais aparentam uma maior confiança na segurança dos seus filhos aquando da utilização da internet, sendo que 69% não estão tão preocupados com a possibilidade de serem vítimas de *cyberbullying*.

No Reino Unido, segundo as conclusões alcançadas num recente inquérito dirigido a 2000 jovens entre os 11 e 18 anos, concluiu-se que um em cada três jovens era vítima de *cyberbullying* através das RSC e de mensagens SMS, sendo que as raparigas eram quatro vezes mais atreitas a serem vítima de tais abusos do que os rapazes.

**2.5.2.** A proteção da privacidade é um dos outros grandes problemas associados à utilização das RSC. Na 30<sup>a</sup> Conferência Internacional das Autoridades de Proteção de Dados e da Privacidade, ocorrida em Estrasburgo entre 15 e 17 de outubro de 2008, foi adotada uma resolução sobre a proteção da privacidade nos serviços de redes sociais, cujas recomendações merecem especial consideração e ponderação<sup>7</sup>. É no seu seguimento e à sua luz que deve ser interpretada a recente evolução que conduziu à mais recente proposta da Comissão para um regulamento e uma diretiva destinados a uma mais efetiva proteção de dados.

**2.5.3.** Também no acordo de autorregulação “Safer Social Networking principles for the EU”, celebrado no dia 10 de fevereiro de 2009<sup>8</sup>, entre os operadores das principais RSC que atuam na Europa, foram claramente identificados os potenciais riscos a que estão expostos os menores de 18 anos que utilizam esses sítios: o assédio (assédio de crianças em sítios internet ou por SMS), a manipulação psicológica (a conquista da amizade de uma criança por um adulto com a intenção de abusar dela sexualmente) e os comportamentos de risco, como a revelação indevida de informações pessoais para finalidades ilícitas.

**2.6.** No âmbito de um Parecer de Iniciativa do CESE, de que fui relator, sobre “O impacto das redes sociais de comunicação e interação na esfera do cidadão/consumidor”<sup>9</sup> foi realizada uma audição com larguíssima participação dos mais representativos interessados na operação e na utilização das RSC,

ONGs e consumidores, para além de representantes do Conselho, da Comissão, da ENISA, da Autoridade Europeia para a Proteção de Dados e de autoridades nacionais interessadas, da qual resultou clara a convergência de pontos de vista entre os representantes da Comissão e da Autoridade Europeia para a Proteção de Dados presentes com a generalidade das sugestões avançadas no referido parecer, para além dos avanços perspectivados no sentido da melhor definição de alguns dos objetivos e da concretização de outros.

2.7. Aí foi particularmente salientada a necessidade de uma harmonização legislativa nos Estados-membros que inclua no mínimo os seguintes aspectos, conforme previstos na Convenção sobre o Cibercrime do Conselho da Europa<sup>10</sup>:

- a) definição do que constitui material pedopornográfico;
- b) definição das vítimas de pedopornografia por referência a crianças com menos de 18 anos;
- c) a posse e o visionamento/carregamento de material pedopornográfico constituem delitos que impõem graves sanções privativas de liberdade.

2.8. Com efeito, embora tenham sido estabelecidas determinadas normas europeias que clarificam as questões jurídicas através de várias recomendações e diretivas, a noção de conteúdos 'prejudiciais' são os conteúdos que os pais, os professores e outros adultos consideram potencialmente nocivos para as crianças. A definição destes conteúdos varia consoante os países e as culturas, podendo incluir a pornografia, a violência, o racismo e a xenofobia, bem como sítios que incitam ao ódio no discurso e na música, ou que tratam de automutilação, de anorexia e de suicídio.

2.9. Só a *Internet Watch Foundation* (Fundação de Observação da Internet) identificou um núcleo de 2.755 sítios internet pedopornográficos domiciliados ao nível internacional em 2007; 80% destes sítios realizam operações comerciais e mudam frequentemente de empresa de acolhimento e de região para evitar serem detectados.

Estas táticas, associadas à natureza multinacional complexa dos crimes, significam que só uma reação mundial unificada que envolva as forças policiais e as autoridades judiciais, os governos e o setor internacional do ambiente em linha permitirá investigar de modo eficaz estes sítios, os seus conteúdos e as organizações que se escondem por detrás deles.

A emergência de novas tecnologias e serviços é fundamental para a inovação e o crescimento das empresas do mundo inteiro

**2.10.** Por conseguinte, a proteção do utilizador, em particular do utilizador vulnerável, especialmente das crianças, mas também o caso de outros públicos mais sensíveis ou vulneráveis, como os idosos, os diminuídos físicos ou psíquicos, é uma prioridade que não deve ser assumida unicamente pelas pessoas encarregadas da sua guarda e educação.

### 3. Inclusão e exclusão social

**3.1.** Entre as principais medidas que já então se consideravam essenciais e que ainda são de atualidade destaca-se a importância de se intensificar o diálogo com os agentes implicados nas RSC, nomeadamente com os jovens, promovendo o seu envolvimento na discussão, concepção e produção de soluções para uma utilização mais segura da internet.

Com efeito, entende-se que os jovens devem ser diretamente implicados na definição dos modelos operacionais, na moderação e na resolução das questões associadas às RSC, porquanto serão provavelmente quem de forma mais eficaz e rápida estará em melhores condições de entender as situações problemáticas que aí surjam.

A criação de um “fórum da juventude” poderia ser útil para a participação dos jovens e para a difusão de informações junto das redes sociais utilizadas pelos grupos mais vulneráveis.

Os jovens têm a sua própria linguagem e muitas vezes manifestam uma certa reticência em ouvir os representantes da autoridade, mas estão abertos aos conselhos dos seus pares no seu meio social. Devem ser tidos em conta os “direitos da criança” e, por conseguinte, os jovens devem participar neste processo.

**3.2.** Julga-se por outro lado que deve ser encarada a criação de um curriculum internacional ou europeu para a formação de conselheiros e terapeutas especializados no acompanhamento das vítimas *online*, nomeadamente nas situações de *bullying* e *grooming* e iniciativas para o aconselhamento em geral e, em particular *online* e o estabelecimento de programas preventivos dirigidos às crianças e adolescentes.

De relevante importância serão também iniciativas em prol da literacia digital, designadamente a utilização segura das RSC, dirigidas não somente às crianças e adolescentes, mas à população em geral, em particular aos pais enquanto encarregados de educação, e às pessoas mais idosas<sup>11</sup>.

**3.3.** Por outro lado, entende-se que os operadores das RSC deverão prosseguir as práticas de autorregulação, em particular no domínio da proteção



dos menores, mas desde que seja assegurada uma monitorização independente do seu efetivo cumprimento, com a possibilidade de padrões mínimos de proteção serem estabelecidos por via legal.

Os organismos de autorregulação da indústria e das partes interessadas têm um conhecimento aprofundado destas tecnologias e têm a possibilidade de desenvolver contramedidas para combater estes abusos. A partilha dos conhecimentos, a sensibilização e identificação dos consumidores para a denúncia dos sítios, bem como a distribuição dos fundos, na medida do possível, para eliminar estes abusos, em particular no contexto da exploração sexual das crianças, constitui um dever essencial da indústria da internet e faz parte integrante da responsabilidade social das empresas deste setor.

Defende-se, aliás, a evolução dos sistemas de autorregulação no sentido da correção, quer a nível comunitário, quer a nível nacional, com a participação das entidades reguladoras por forma a ser garantido um efetivo cumprimento dos acordos celebrados, a prevenção dos desvios, o sancionamento das infrações e a punição dos transgressores pelos seus pares.

**3.4.** Entende-se ainda que esforços adicionais são necessários no sentido de reforçar a informação e de aprofundar a educação desde os primeiros anos escolares, com vista a uma maior prevenção dos riscos e a uma melhor utilização destes locais de socialização, para o que deverão ser lançadas campanhas de sensibilização a nível comunitário e nos diferentes Estados-membros.

Neste sentido julga-se que seria da maior utilidade um *eYouGuide* especificamente orientado para os utilizadores das RSC, uma espécie de portal dos direitos do utilizador dos serviços de RSC, com a possibilidade da denúncia de abusos e de resolução de conflitos ao nível pan-europeu, ou seja um único sítio onde fosse possível “gerir” os direitos dos utilizadores, avaliar a coordenação comunitária, discutir formas de intervenções e políticas e apreciar a cooperação entre as autoridades nacionais.

Julga-se também que os programas de investigação e desenvolvimento, nacionais e comunitários, e os próprios operadores devem investir mais no desenvolvimento e no aperfeiçoamento de instrumentos técnicos de filtragem de acessos e de bloqueamento, que permitam às famílias uma aplicação prudente, mas consistente, do princípio da precaução.

**3.5.** Atenta a natureza do fenómeno e o seu carácter evolutivo e dinâmico, era importante que um Livro Verde da Comissão ponderasse as mais recentes evoluções neste domínio e definisse as principais opções para os desenvolvimentos futuros, analisando os respectivos impactos, com alargada audição das várias empresas, profissionais, estudiosos e organizações e associações da sociedade civil interessadas.

Nesse âmbito julga-se que seria de encarar a possibilidade de um quadro legal consistente em toda a UE, saído de uma maior cooperação e coordenação das políticas nacionais. Aspecto a merecer uma atenção especial será o das condições contratuais de adesão às redes, onde as cláusulas abusivas são a regra, designadamente no que respeita à lei aplicável e ao foro competente.

**3.6.** A criação de uma plataforma ao nível da UE, que incluía as empresas, os governos, as instituições bancárias e financeiras, os gestores de cartões de crédito, as ONGs e os representantes do setor da educação, do patronato e dos trabalhadores, poderia constituir um instrumento valioso para uma análise e ação rápidas em toda a União, com uma difusão da informação que ultrapasse as fronteiras da UE para facilitar a cooperação policial e judiciária internacional.

**3.7.** Também o estabelecimento de um “centro de colocação em rede” ao nível da Comissão, que procederia a investigações sobre projetos realizados não só na Europa, mas também no resto do mundo, deveria apoiar a plataforma para garantir a atualização e a pertinência dos conhecimentos, incluindo das estatísticas, bem como a difusão de métodos eficazes para combater os problemas e a sua rápida transmissão aos parceiros ativos. O papel principal deste centro seria reagir aos novos desafios acompanhando o ritmo da sua evolução.

**3.8.** Mas, porque se trata essencialmente de um fenómeno internacional, encontrando-se os principais serviços de RSC sujeitos a jurisdições fora do espaço da UE, considera-se essencial a promoção efetiva das seguintes medidas:

1. A definição de princípios e regras de conduta dos serviços de RSC, em particular os serviços dirigidos a menores, num plano internacional.

2. A institucionalização de mecanismos de supervisão do cumprimento de tais regras, que dada a natureza dos serviços deverá ser forçosamente de âmbito transfronteiriço.

3. O reforço e agilização da cooperação da União Europeia com os países terceiros, europeus e não europeus, a um nível político e operacional, na identificação dos riscos e problemas associados à utilização das RSC, na procura das melhores soluções para fazer face a tais situações, e sempre que o quadro legal internacional o permita na remoção efetiva das situações lesivas dos direitos dos cidadãos/ consumidores.

4. A necessidade de uma efetiva cooperação e coordenação internacional entre as várias partes interessadas, de modo a maximizar o efeito das medidas necessárias em prol de uma utilização mais segura da internet, sendo necessária uma abordagem internacional mais atuante para garantir a difusão e troca de conhecimentos, a coordenação da feitura e da aplicação das leis e a obtenção

de financiamento para a implementação das medidas necessárias, nos planos interno e externo da UE.

5. A necessidade dos Estados-membros ratificarem as Convenções do Conselho da Europa sobre o *cybercrime* e a proteção das crianças contra a exploração sexual e abuso sexual<sup>12</sup>, o que constituirá um passo importante para a União Europeia poder atuar na cena internacional como um bloco coeso.

**3.9.** Pela mesma razão entende-se que apenas com uma abordagem harmonizada e integrada a nível internacional da regulamentação relativa aos serviços audiovisuais será possível implementar eficazmente quaisquer medidas de proteção, em particular no que se refere aos aspectos dos sistemas de classificação e dos software de filtragem dos conteúdos, da clarificação das questões da responsabilidade pelos conteúdos ilícitos e lesivos, pelo que se apela a uma maior cooperação e coordenação entre as organizações europeias e internacionais e renova a sua proposta da criação de um quadro internacional de códigos de conduta, diretivas e medidas básicas para adequada proteção dos menores e da dignidade humana.

**3.10.** Pondera-se, ainda, a vantagem do alargamento e da integração das competências hoje dispersas por várias entidades no sentido da criação de um Provedor (Ombudsman) a nível comunitário para todas as questões ligadas com o audiovisual – privacidade, proteção de dados, dignidade humana, direito de resposta, liberdade de expressão – abrangendo as RSC, à semelhança, em termos de direito comparado, do modelo canadiano do *Privacy Commissioner*, cuja intervenção, no âmbito dos seus poderes alargados, em relação ao Facebook por alegada retenção indevida de dados pessoais, fez recentes notícias<sup>13</sup>.

## **4. Antigos e novos direitos fundamentais: riscos acrescidos e proteção reforçada**

**4.1.** Estes desenvolvimentos fomentaram a necessidade de uma reflexão aprofundada sobre o seu enquadramento jurídico a nível comunitário, com a definição de novos direitos e novas formas de proteção.

Já em fevereiro de 2005, em parecer do Comité Económico e Social Europeu sobre a “Proposta de recomendação do Parlamento Europeu e do Conselho relativa à proteção dos menores e da dignidade humana e ao direito de resposta em relação ao desenvolvimento da competitividade da indústria europeia de serviços audiovisuais e de informação”<sup>14</sup>, enquanto seu relator, tive a oportunidade de salientar que os desafios colocados pelos recentes desenvolvimentos tecnológicos,

de que se destacam o aumento da potência e da capacidade de armazenamento dos computadores e o fato de as tecnologias de banda larga permitirem a distribuição de conteúdos, como sejam os vídeos nos telemóveis de 3ª geração, e, por outro lado, as preocupações manifestadas pelos cidadãos em geral e, em particular, pelos pais e responsáveis de educação, pela indústria e pelos reguladores, no que se refere à proliferação de conteúdos e comportamentos ilegais, lesivos e indesejáveis em todas as formas de teledifusão, desde a radiodifusão à internet, impunham a criação de condições legais ou outras que propiciem um clima de maior segurança, certeza e proteção que incentivasse o desenvolvimento das novas tecnologias de informação num ambiente que:

a) promovesse iniciativas com vista a facilitar um acesso mais vasto dos menores aos serviços audiovisuais e de informação, com garantias de segurança e controle dos conteúdos dos programas, evitando simultaneamente conteúdos potencialmente lesivos, incluindo uma harmonização “ascendente” através da colaboração entre os organismos de autorregulação e de correção dos Estados-membros e do intercâmbio de melhores práticas em várias questões, entre elas um sistema de símbolos descritivos comuns que auxilie os espectadores a avaliar o conteúdo dos programas;

b) permitisse aos menores uma utilização responsável dos novos serviços audiovisuais e de informação em linha, nomeadamente por uma maior sensibilização dos pais, educadores e professores para o potencial dos novos serviços e para os meios adequados de proteção dos menores, em particular através das competências relacionadas com os meios de comunicação ou de programas educativos nesse domínio;

c) facilitasse a identificação e o acesso a conteúdos e serviços de qualidade para menores, designadamente pelo fornecimento de meios de acesso nos estabelecimentos de ensino e nos locais públicos;

d) incentivasse a indústria a evitar e a combater qualquer tipo de discriminação baseada no sexo, raça ou origem étnica, religião ou crença, deficiência, idade ou orientação sexual em todos os meios de comunicação.

**4.2.** Vários outros aspectos visando promover uma utilização mais segura da internet devem ainda ser considerados como desejáveis recomendações aos Estados-membros, como sejam, em particular:

a) uma maior formação e informação sobre os meios de garantir uma maior segurança na utilização da internet;

b) a responsabilização dos fornecedores de espaços e de acessos e a sua obrigação de acatar de imediato qualquer decisão de autoridade legítima que ordene a cessação de transmissão de programas ou de conteúdos ilegais, nocivos ou prejudiciais;

c) o incitamento e o apoio ao desenvolvimento de *hotlines*, de tecnologias de filtragem, de classificação de conteúdos, de medidas de luta contra o spam e o spim;

d) a responsabilização dos autores de meios informáticos de acesso à internet e de sistemas de exploração de servidores pela defesa e preservação dos sistemas vendidos contra os ataques de vírus, com a obrigação de oferecer meios fáceis e acessíveis de luta antivírus;

e) implementação de sistemas de identificação e de informação sobre os conteúdos nocivos e prejudiciais e a retirada de todos os conteúdos de caráter racista, xenófobo ou que façam a apologia do crime, da violência ou do ódio.

**4.3.** A particular preocupação refletida no que se refere à utilização da internet não deve no entanto ser entendida como menor atenção a ser dada em relação a todos os meios tradicionais de comunicação social, em particular a radiodifusão sonora e televisiva, onde ofensas graves a públicos sensíveis, designadamente a menores, devem ser objeto de uma especial atuação seja por via da autorregulação seja da heterorregulação.

Merecem, pois uma particular atenção todas as medidas que:

a) encorajem os *media* (mídia) a adotar regras de deontologia precisas e concretas com vista a assegurar o respeito devido pela vida privada;

b) incitem os *media* a criar mecanismos de autorregulação perante os quais as vítimas de atentados à vida privada e à dignidade humana possam apresentar as suas queixas;

c) criem órgãos independentes, incluindo de natureza judicial, para exame deste tipo de queixas se os mecanismos de autorregulação se revelarem inoperantes;

d) instaurem um direito à indenização dos prejuízos materiais e morais com função simultaneamente reparadora para as vítimas e dissuasória para os responsáveis por atentados graves e sistemáticos à vida privada e à dignidade das pessoas;

e) procedam a um acompanhamento das emissões de conteúdos que possam constituir atentados à vida privada, à dignidade humana e aos direitos fundamentais.

**4.4.** Um dos domínios a merecer um lugar destacado nas nossas preocupações é, claramente, o da proteção dos dados e está na origem da

Constata-se que 54% dos pais europeus estão preocupados com a possibilidade dos seus filhos poderem ser vítimas de *cyberbullying*

mais recente proposta de regulamento da Comissão Europeia relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados)<sup>15</sup>.

**4.4.1.** Dando-se acerbamente conta da rápida evolução tecnológica e dos novos desafios em matéria de proteção de dados pessoais, consequência do aumento espetacular da utilização de dados pessoais numa escala sem precedentes e de que as pessoas disponibilizam cada vez mais as suas informações pessoais de uma forma pública e global, a Comissão constatou que o atual quadro jurídico não permitiu evitar uma fragmentação na execução da proteção dos dados pessoais na União Europeia, nem a insegurança jurídica e o sentimento generalizado na opinião pública de que subsistem riscos significativos, particularmente nas atividades em linha.

Nesse sentido a Comissão acaba de propor a adoção de um novo quadro jurídico de proteção dos dados mais sólido e coerente apoiado por uma aplicação rigorosa das regras, que permita à economia digital desenvolver-se em todo o mercado interno, às pessoas singulares controlar os seus próprios dados, bem como reforçar a segurança jurídica e prática para os operadores económicos e as entidades públicas.

**4.4.2.** Entre os elementos mais salientes desta Proposta de Regulamento destacam-se:

*a) Uma nova base jurídica*

A presente proposta baseia-se no artigo 16º do TFUE, que constitui a nova base jurídica para a adoção das regras em matéria de proteção de dados introduzidas pelo Tratado de Lisboa e permite a adoção de regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelos Estados-membros no exercício de atividades abrangidas pelo direito da União.

Permite igualmente a adoção de regras relacionadas com a livre circulação de dados pessoais, incluindo os dados pessoais tratados pelos Estados-membros ou por entidades privadas.

Por seu turno um regulamento é o instrumento jurídico mais adequado para definir o quadro da proteção de dados pessoais na União. A sua aplicabilidade direta, prevista no artigo 288º do TFUE, permitirá reduzir a fragmentação jurídica e proporcionar maior segurança jurídica, introduzindo um conjunto harmonizado de regras de base, melhorando a proteção dos direitos fundamentais das pessoas singulares e contribuindo para o bom funcionamento do mercado interno.

### *b) A sua consideração ao nível dos direitos fundamentais*

O direito à proteção de dados pessoais está consagrado no artigo 8º da Carta dos Direitos Fundamentais da UE, no artigo 16º do TFUE e no artigo 8º da CEDH. Conforme salientado pelo Tribunal de Justiça da UE, o direito à proteção de dados pessoais não é absoluto, mas deve ser considerado em relação à sua função na sociedade.

A proteção de dados está profundamente relacionada com o respeito pela vida privada e familiar, protegido pelo artigo 7º da Carta. Os outros direitos fundamentais consagrados na Carta suscetíveis de serem afetados são a liberdade de expressão (artigo 11º da Carta), a liberdade de empresa (artigo 16º), o direito à propriedade e, em especial, a proteção da propriedade intelectual (artigo 17º, n. 2), a proibição de discriminação em razão da raça, origem étnica, características genéticas, religião ou convicções, opiniões políticas ou outras, deficiência ou orientação sexual (artigo 21º), os direitos da criança (artigo 24º), o direito a um elevado nível de proteção da saúde humana (artigo 35º); o direito de acesso aos documentos (artigo 42º); o direito à ação e a um tribunal imparcial (artigo 47º).

### *c) Novos princípios*

Os novos elementos acrescentados são, em especial, o princípio da transparência, a clarificação do princípio da minimização de dados e a instauração das obrigações e da responsabilidade global do responsável pelo tratamento.

São, assim, clarificadas as condições para que o consentimento seja válido enquanto fundamento jurídico para o tratamento lícito (artigo 7º); estabelecidas condições suplementares para a licitude do tratamento de dados pessoais de crianças em relação a serviços da sociedade da informação que lhes são diretamente propostos (artigo 8º); genericamente prevista uma proibição geral de tratamento de categorias especiais de dados pessoais e as exceções a esta regra geral (artigo 9º); e clarificado que o responsável pelo tratamento não é obrigado a obter informações adicionais para identificar o titular dos dados para efeitos exclusivos do respeito de qualquer disposição do presente regulamento (artigo 10º).

### *d) Novos direitos do titular dos dados*

São, enfim, estabelecidos novos e importantes direitos do titular dos dados, de que se destacam:

#### *1 – Transparência*

O artigo 11º introduz a obrigação de os responsáveis pelo tratamento fornecerem informações transparentes, de fácil acesso e compreensão.

O artigo 12º obriga o responsável pelo tratamento a prever procedimentos e mecanismos para o exercício dos direitos pelo titular dos dados, incluindo

meios para pedidos por via eletrônica que requeiram resposta à pessoa em causa dentro de um prazo fixado e os motivos da recusa.

#### *2 – Informações e acesso aos dados*

O artigo 14º descreve mais pormenorizadamente as obrigações de informação pelo responsável pelo tratamento para com o titular dos dados e acrescenta informações suplementares, incluindo sobre o período de conservação, o direito de apresentar queixa, as transferências internacionais e a fonte de origem dos dados.

O artigo 15º prevê o direito de acesso do titular de dados aos seus dados pessoais, com base no artigo 12º, alínea *a*), da Diretiva 95/46/CE, e acrescenta novos elementos, tais como prever a informação aos titulares dos dados sobre o período de conservação, os direitos de retificação, de apagamento e de apresentação de queixa

#### *3 – Retificação e apagamento*

O artigo 16º estabelece o direito do titular dos dados à retificação.

O artigo 17º confere ao titular dos dados o direito a ser esquecido e ao apagamento, e prevê as condições do direito a ser esquecido, incluindo a obrigação do responsável pelo tratamento que tornou públicos os dados pessoais de informar os terceiros sobre o pedido da pessoa em causa de apagamento de quaisquer ligações para esses dados, ou cópias ou reproduções que tenham sido efetuadas.

O artigo 18º introduz o direito do titular dos dados à portabilidade dos dados, ou seja, de transferir dados de um sistema de tratamento eletrônico para outro, sem que o responsável pelo tratamento se possa opor.

Como condição prévia, e para melhorar o acesso das pessoas

singulares aos dados pessoais que lhe dizem respeito, prevê o direito de obter esses dados do responsável pelo tratamento num formato eletrônico estruturado e de utilização corrente.

#### *4 – Direito de oposição e de definição de perfis*

O artigo 19º confere ao titular dos dados o direito de oposição da Diretiva 95/46/CE, com algumas inovações, designadamente quanto ao ónus da prova e da sua aplicação à comercialização direta.

O artigo 20º é relativo ao direito de o titular dos dados não ser objeto de uma medida com base na definição de perfis e tem em consideração a recomendação do Conselho da Europa sobre a definição de perfis.

#### *5 – Vias de recurso, responsabilidade e sanções*

Os artigos 73º e sgs. preveem o direito de qualquer titular de dados apresentar queixa a uma autoridade de controlo: especificam os organismos,



organizações ou associações que podem apresentar queixa em nome do titular dos dados ou, em caso de violação de dados pessoais, independentemente da queixa apresentada por um titular de dados; definem o direito de recorrer aos tribunais contra uma autoridade de controlo e preveem, especificamente, uma ação judicial a fim de obrigar a autoridade de controlo a dar seguimento a uma queixa, clarificando a competência dos tribunais do Estado-membro em que esteja estabelecida a autoridade de controlo.

Preveem também que a autoridade de controlo do Estado-membro onde resida o titular dos dados possa intentar, em nome deste último, uma ação junto dos tribunais de outro Estado-membro onde esteja estabelecida a autoridade de controlo competente.

Estabelecem regras gerais para os processos judiciais, incluindo o direito de organismos, organizações ou associações representarem os titulares de dados junto dos tribunais, o direito das autoridades de controlo de intervirem em processos judiciais e de informar os tribunais sobre processos paralelos noutro Estado-membro, bem como a possibilidade de os tribunais suspenderem, nesse caso, a instância 38. Os Estados-membros são obrigados a assegurar ações judiciais rápidas.

A proteção da  
privacidade é  
um dos outros  
grandes problemas  
associados à  
utilização das RSC

O artigo 77º diz respeito ao direito de indenização e à responsabilidade tornando este direito extensível aos danos causados pelos subcontratantes e clarifica a responsabilidade dos responsáveis conjuntos pelo tratamento e dos subcontratantes.

Finalmente os artigos 78º e 79º obrigam os Estados-membros a estabelecerem regras sobre sanções aplicáveis às infrações ao regulamento e a assegurar a sua execução e obrigam cada autoridade de controlo a sancionar as infrações administrativas mediante multas até um determinado montante máximo, em função de circunstâncias concretas.

#### *6 – Disposições relativas a situações específicas de tratamento de dados*

Os artigos 80º e sgs. tratam da compatibilização do direito à proteção de dados com outros direitos fundamentais e obrigam designadamente os Estados-membros a adotarem isenções e derrogações a disposições específicas do regulamento sempre que necessário para conciliar o direito à proteção de dados pessoais com o direito à liberdade de expressão; a assegurar garantias específicas para o tratamento de dados no domínio da saúde; a adotarem legislação específica para o tratamento de dados pessoais no domínio do

emprego ou para o tratamento de dados pessoais para efeitos de investigação histórica, estatística e científica.

O artigo 84º autoriza os Estados-membros a adotarem regras específicas sobre o acesso de autoridades de controlo a dados pessoais e a instalações, sempre que os responsáveis pelo tratamento dos dados estiverem sujeitos a obrigações de confidencialidade e o artigo 85º autoriza as igrejas, por força do artigo 17º do Tratado sobre o Funcionamento da União Europeia, a continuarem a aplicar um conjunto completo de regras de proteção de dados, se forem adaptadas ao presente regulamento.

## Notas

<sup>1</sup> [http://www.saferinternet.org/ww/en/pub/insafe/safety\\_issues/faqs/social\\_networking.htm](http://www.saferinternet.org/ww/en/pub/insafe/safety_issues/faqs/social_networking.htm)

<sup>2</sup> IP/09/232 Bruxelas, 10 de fevereiro de 2009.

<sup>3</sup> Sobre este ponto, ver em particular, o Relatório da ENISA (European Network and Information Security Agency) “Security Issues and Recommendations for Online Social Networks” em <[www.enisa.europa.eu/doc/pdf/deliverables/enisa\\_pp\\_social\\_networks.pdf](http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf)>

<sup>4</sup> [http://ec.europa.eu/information\\_society/activities/sip/policy/consultations/ageverif\\_sns/index\\_en.htm](http://ec.europa.eu/information_society/activities/sip/policy/consultations/ageverif_sns/index_en.htm)

<sup>5</sup> [http://ec.europa.eu/information\\_society/activities/sip/docs/pub\\_consult\\_age\\_rating\\_sns/summary\\_report.pdf](http://ec.europa.eu/information_society/activities/sip/docs/pub_consult_age_rating_sns/summary_report.pdf)

<sup>6</sup> Flash Eurobarometer survey 2008: Towards a Safer Use of the Internet for children in the EU – a parents’ perspective, [http://ec.europa.eu/public\\_opinion/flash/fl\\_248\\_en.pdf](http://ec.europa.eu/public_opinion/flash/fl_248_en.pdf)

<sup>7</sup> Resolution on Privacy Protection in Social Network Services, [http://www.privacyconference2008.org/adopted\\_resolutions/STRASBOURG2008/resolution\\_social\\_networks\\_en.pdf](http://www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_social_networks_en.pdf)

<sup>8</sup> “Safer Social Networking principles for the EU”, disponível em [http://ec.europa.eu/information\\_society/activities/social\\_networking/eu\\_action/selfreg/index\\_en.htm#self\\_decl](http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm#self_decl)

<sup>9</sup> Parecer CESE 1697/2009, TEN/390 de 4 de Novembro de 2009

<sup>10</sup> Convenção sobre o Cibercrime ETS 185 do Conselho da Europa, de 23.11.2001.

<http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

<sup>11</sup> Sobre este tema importa referir o Parecer exploratório do Comité Económico e Social Europeu sobre “Melhorar a literacia, as competências e a inclusão digitais” de que foi relatora Laure Batut (TEN/453 – CESE 1182/2011 de 13 de Julho de 2011), de cujas conclusões, pela sua importância, se respigam as seguintes:

*‘1.3 A info-inclusão ou inclusão digital deve constituir uma abordagem global e garantir, através do ambiente digital, a emancipação de todos, qualquer que seja a sua situação na sociedade. O CESE considera que a União e os Estados-membros deveriam garantir a acessibilidade do ambiente digital através da aprendizagem constante das competências digitais para exercer uma profissão, para efeitos de realização pessoal e para exercer o direito de cidadania.*

1.4 O acesso à infraestrutura e às ferramentas deve ser direito fundamental da pessoa humana.

1.8 De um modo geral, o CESE considera conveniente:

- fazer da info-inclusão um elemento de mainstreaming das políticas, ao nível da UE e dos Estados-membros;
- concluir rapidamente as infraestruturas de redes (regiões isoladas, banda larga, etc.);
- conceber, desde o início, como inclusivas e não discriminatórias as políticas públicas em matéria de desenvolvimento do ambiente digital, aos níveis europeu, nacional e local;

– favorecer a utilização de materiais e programas informáticos recentemente desatualizados;

– disponibilizar meios para garantir a info-inclusão das mulheres.

1.8.3 Para promover a segurança de públicos vulneráveis face ao ambiente digital:

- definir conteúdos de base da Internet, sem deixar tudo entregue ao mercado (UE e Estados-membros);
- definir normas “antipoluição” dos sítios Web e ensinar a segurança digital desde os bancos da escola;
- garantir que todos os sítios Web contenham dispositivos que alertem o utilizador para procedimentos de segurança elementares;

– garantir a criação e o respeito pelos direitos do utilizador das redes;

– para o efeito, estabelecer um código do direito dos utilizadores do ambiente digital, em conformidade com os princípios da Carta dos Direitos Fundamentais e com o artigo 9.º do Tratado, garantindo, pelo menos, o respeito pela liberdade de expressão e de informação, o direito à proteção dos dados pessoais, o direito ao esquecimento e o direito à proteção dos menores.

1.8.5 No plano da educação inclusiva para todos, o CESE preconiza que a União se comprometa a:

- promover a igualdade de acesso a uma educação inclusiva em todas as escolas;
- promover a info-inclusão do futuro desde a idade pré-escolar, sem discriminações;
- promover a formação digital de pais e professores e a reorganização das condições de trabalho destes últimos;
- promover, para os alunos, e sobretudo para os alunos com dificuldades escolares, a generalização da prática do digital na escola, designadamente de forma lúdica, enquadrada, como é óbvio, pelos professores, para uma utilização controlada da força das imagens, que requer novas formas de aprendizagem e de expressão, designadamente lúdicas (utilização de smartphones na sala de aula, de ‘jogos sérios’, de tablets, de livros digitais, das redes sociais, etc.);

– promover a abertura para todos do acesso ao mercado de trabalho através da aquisição de bases sólidas, tanto gerais como digitais.’

<sup>12</sup> <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=201&CL=ENG>

<sup>13</sup> Ver [http://www.priv.gc.ca/aboutUs/mm\\_e.cfm#contenttop](http://www.priv.gc.ca/aboutUs/mm_e.cfm#contenttop), a propósito do Office of the Privacy Commissioner of Canada (OPC) e sobre a sua recente intervenção relativamente ao Facebook ver, [http://www.priv.gc.ca/media/nr/-c/2009/nr-c\\_090716\\_e.cfm](http://www.priv.gc.ca/media/nr/-c/2009/nr-c_090716_e.cfm)

<sup>14</sup> Parecer TEN/195, de 17 de Fevereiro de 2005.

<sup>15</sup> COM(2012) 11 final de 25.1.2012.

