FACULDADE DE DIREITO DA UNIVERSIDADE NOVA DE LISBOA

MESTRADO EM DIREITO 2011/2012

Direito da Comunicação

Docente: Professora Doutora Mª Eduarda Gonçalves

Discentes: Joana Veríssimo 002706

Maria Macias 002721

Sofia Rodrigues 002702

IMPLICAÇÕES JURÍDICAS DAS REDES SOCIAIS NA INTERNET: UM NOVO CONCEITO DE PRIVACIDADE?

ÍNDICE

INTRODUÇÃO

No nosso trabalho procuramos entender o impacto jurídico das redes sociais *online*. Começaremos por definir e caracterizar estas redes e observar o seu impacto sociocultural. Passaremos depois à análise do impacto jurídico das mesmas. Concentrar-nos-emos em alguns dos problemas criados ou potenciados por esta nova realidade: no plano do direito laboral e penal, nas questões que surgem no que toca à participação das crianças nestas redes e na reformulação do conceito jurídico clássico de privacidade. Finalmente, apresentaremos as vias que têm sido apresentadas como possíveis maneiras de lidar com esta nova realidade: a auto-regulação e a hetero-regulação.

O IMPACTO JURÍDICO DAS REDES SOCIAIS NA INTERNET

1. Conceito de redes sociais

As redes sociais são um fenómeno inerente à natureza social do homem. Estas correspondem a pequenas comunidades, que se formam entre os membros de grandes sociedades, e surgem quando se criam grupos que partilham valores, interesses ou objectivos. Estas partilhas aproximam as pessoas que formam, entre si, laços sociais que as unem. Este aspecto agregador faz com que estas pequenas comunidades contribuam para a sanidade das grandes sociedades em que se inserem pois fomentam sentimentos de pertença e solidariedade.

Estas redes podem manifestar-se de maneiras diferentes e em plataformas diferentes acompanhando o desenvolvimento social e tecnológico. Os clubes de futebol, igrejas e clubes de livros são exemplos de redes sociais. Recentemente surgiram as redes socias online. As características do espaço cibernético fazem dele a plataforma ideal para estas redes sociais visto que a internet é um espaço sem fronteiras, com liberdade de entrada e circulação, com utilizadores em todo o mundo que podem, mais facilmente, comunicar entre si com grande rapidez, quer por escrito quer via *webcam*.

Para efeitos do presente trabalho teremos como referência a seguinte noção: "*Uma rede social é uma estrutura social composta por pessoas ou organizações, conectadas por um ou vários tipos de interesses e que partilham valores e objectivos. Estas Redes tendem a estar articuladas com as*

Novas Tecnologias de Informação podendo assentar numa plataforma online onde se estruturam estas relações sociais entre utilizadores."[1]

a. Redes Sociais Online

As redes sociais *online* surgiram na primeira década do século XXI e a sua expansão e cimentação no nosso quotidiano é tal que ao nos referirmo-nos a redes socias automaticamente pensamos em redes socias online. Estas surgiram quando se sentiu necessidade de criar uma ferramenta de comunicação mais abrangente, imediata e que permitisse contactar indivíduos sem ser necessário ter o seu endereço electrónico. Assim, em 1997 surge a primeira rede social, o *Sixdegrees*. É com o *Sixdegrees* que nasce o fenómeno das redes socias *online* pois as suas características permitiam a inserção dos utilizadores numa comunidade, em que se apresentavam através do seu perfil e comunicavam com terceiros utilizadores. Em 2003 o *Myspace* bate recordes de adesão e capta a atenção de empresas que se apercebem do potencial comercial destas redes. O *Myspace* apostou na interactividade criando espaços de publicação de músicas, fotos e um *blog* para cada usuário, tornando-se numa das redes sociais mais populares do mundo. Durante estes anos vão surgindo diversas redes com temáticas diversas, desde as redes sociais com intuitos profissionais (*Linkedin*), académicos (*Academia.edu*) ou turísticos (*Couchsurfing*). Finalmente, em 2004 surge o *Facebook*. O seu conceito é muito semelhante aos das restantes redes socias mas a criatividade dos seus criadores centrou-se na elaboração de aplicações que permitissem aprofundar as ligações entre utilizadores. Em Janeiro de 2009 um estudo[2] concluiu que o *Facebook* é a rede social com maior número de frequentadores mensais de toda a internet.

b. Características e finalidades

Todas estas redes possuem características e propósitos muito semelhantes: são *user based*, ou seja, ao contrário das normais páginas na web, baseiam-se nos utilizadores, e não no conteúdo, isto significa que os utilizadores são o centro da Rede e são eles que lhe conferem vida; criam um sentimento de comunidade, e, para servir este propósito são definidos temas que deverão aliciar os futuros utilizadores a criarem um perfil; permitem a criação de relações entre utilizadores, ou seja, não basta que a rede tenha muitos utilizadores, para se criar uma comunidade, estes utilizadores devem interagir entre si, formando laços de amizade; é um sistema aberto, o que se traduz numa relativa liberdade de adesão e de circulação na rede, apenas limitada pelas definições de privacidade

[1] Conceito retirado de http://pt.wikipedia.org/wiki/Rede_social.
[2] Estudo consultado em http://siteanalytics.compete.com/facebook.com/, a 16 de Abril de 2012.

da própria rede o que garante o crescimento da comunidade; e, finalmente, é uma rede descentralizada, ou seja, os utilizadores encontram-se todos no mesmo plano, sujeitos às mesmas regras e com liberdade de personalizar o seu espaço na rede. As suas relações desenrolam-se no plano horizontal sem qualquer relação hierárquica.

Apesar de este ser um fenómeno ainda jovem, que se desenvolveu na primeira década do século XXI, já todos constatámos o impacto socio-cultural e jurídico que estas tiveram. Estão presentes no nosso quotidiano e mudaram os nossos hábitos, desde a forma como comunicamos, socializamos, consultamos as notícias, pesquisamos e até arranjamos emprego.[3]

Dos 625 milhões de utilizadores activos da internet cerca de 57% desses utilizadores criaram perfis em redes sociais. Em Portugal o impacto das redes é ainda mais significativo pois dos 2,9 milhões de utilizadores activos da internet, cerca de 2,1 milhões criaram um perfil numa rede social, ou seja, cerca de 73%, um valor superior à média mundial. A actividade principal nas redes sociais dos utilizadores portugueses é a partilha fotos (70,48%).[4]

Estes números são expressivos da infiltração destas redes na vida dos utilizadores da internet. O resultado desta implantação das redes sociais no nosso quotidiano pode observar-se nalgumas modificações socioculturais.

Estas novas plataformas de partilha permitiram impulsionar o jornalismo de cidadão.[5] Outro foi ainda o papel destas redes na "Primavera Árabe", as redes sociais foram verdadeiros "palcos" utilizados pelos cidadãos descontentes para difundirem as suas mensagens políticas e apelarem à revolta, visto que não o podiam fazer publicamente devido à natureza repressiva dos regimes em causa. [6]

---

[3] Prova deste impacto é a reformulação da clássica teoria dos seis graus de separação. Em 2011 a Universidade de Milão em conjunto com o Facebook realizou um estudo para pôr à prova esta teoria. O estudo concluiu que estamos cada vez mais próximos apenas separados por 4,74 graus. A razão encontrada para o menor grau de separação foram as ligações estabelecidas pelas redes sociais que conectam os seus utilizadores e são cada vez mais populares em todo o mundo.

[4] Estudo da UM's WAVE *research into the phenomenal growth of social media is the most robust data set in the world*, consultado em www.universalmccann.bitecp.com/wave4/Wave4.pdf, a 16 de Abril de 2012.

[5] O cidadão comum ocupou o lugar do jornalista ao dispor de um telemóvel ou camara fotográfica, de uma ligação à internet e uma conta numa rede social consegue partilhar com o mundo inteiro os acontecimentos presenciados em primeira mão. Recentemente observámos este fenómeno com a "Primavera Árabe" em que as noticias das revoltas que se estavam a dar chegavam ao mundo através dos relatos dos cidadãos dos países revoltos que publicavam vídeos e fotografias dos ataques e da destruição nas suas contas em redes sociais como o Youtube. Esta possibilidade de comunicação foi muito importante pois estes países não permitiam a entrada de jornalistas numa tentativa de reprimir e camuflar as revoltas.

[6] Em Portugal a manifestação "Geração à rasca", que em Março de 2011 reuniu cerca de 200 mil pessoas em várias capitais de distrito, foi organizada através da rede social Facebook.

O nível de popularidade destas redes e o facto de a adesão a estas ser totalmente gratuita significa que estas são plataformas ideais para a disseminação de mensagens publicitárias e solidárias. As marcas e empresas aperceberam-se do potencial de divulgação de produtos nestas redes e agora não dispensam a criação de perfis para auto-promoção. Do mesmo modo, as organizações recorrem às redes para promoverem as suas causas e angariarem fundos.

2. Impacto Negativo das Redes Sociais – "Novos Perigos"

a) Perfis Falsos

Se uma das grandes revoluções da era digital foi a criação de redes sociais virtuais que vieram alterar por completo a forma de convivência em sociedade, por outro lado, a extrema acessibilidade às mesmas e a facilidade com que se cria uma página, fomentaram problemas como a excessiva exposição ao mundo virtual ou a tentação de se refugiar num mundo paralelo. Mas o verdadeiro e grande problema surge quando um usuário resolve se fazer passar por outra pessoa, criando uma página com um perfil que não é o seu, conduta extremamente simples de ser praticada no meio electrónico, uma vez que basta copiar a fotografia de outra pessoa e criar o perfil com o nome desta, sem que haja por parte das empresas que gerem os *websites* das redes sociais qualquer tipo de autenticação de identidade. Assim, um utilizador mal-intencionado facilmente cria uma página com dados falsos para atrair um determinado tipo de pessoas a fim de as importunar, enganar, explorar, difamar ou, no limite, levá-las ao suicídio. A este responsável usualmente se atribui o nome "*fake*".

Todos (os utilizadores) estamos vulneráveis a este tipo de situações, 24 sobre 24 horas, 7 dias por semana. E vários são os casos em que são criados perfis falsos em nome de alguém com o objectivo de ofender a sua honra e o seu bom nome. As vítimas são, normalmente, figuras públicas, políticos ou alguém conhecido dentro de um círculo de amizades. Um caso conhecido foi o da actriz brasileira Débora Borges que foi perseguida por um perfil falso no *Twitter*, com o intuito de denegrir a sua imagem perante amigos e familiares, inventar histórias do seu dia-a-dia, ou até manter conversações com outras celebridades[7]. Mas os exemplos não se ficam por aqui. Há casos em que ex-namorados, accionados por motivações interiores de raiva e frustração, criam um perfil falso com o objectivo de se vingar, transmitindo ideias erradas sobre o seu ex-parceiro, sobre as suas escolhas na carreira, no estilo de vida, para simplesmente o importunar ou até com o intuito de lhe arruinar a

[7]http://ego.globo.com/Gente/Noticias/0,,MUL1638305-9798,00-BARBARA+BORGES+E+PERSEGUIDA+POR+PERFIL+FALSO+NO+TWITTER.html. Acesso a 30 de Abril de 2012.

vida[8]. Outras situações há em que um grupo de amigos, que frequentam a mesma turma, cria um perfil falso de uma das suas professoras, a título de brincadeira, mas que pode tomar contornos graves. Os molestadores de crianças, que criam páginas de perfil, fazendo-se passar por jovens com determinados interesses, a fim de se aproximarem de uma criança vulnerável e a levarem a tomar determinadas atitudes, ou a marcar encontros com as mesmas, constituem outro exemplo. E há situações ainda mais graves em que a pressão e a persuasão de quem cria o perfil é de tal ordem, e a vítima está de tal forma perturbada, que a humilhação por que passa chega mesmo a resultar em suicídio.

Em género de síntese, a criação dos "*fakes*" manifesta-se de duas formas distintas: o utilizador, com a intenção de buscar o anonimato para abordar terceiros, faz-se passar por uma pessoa fictícia, através da escolha de uma imagem de uma pessoa desconhecida para atribuí-la ao seu perfil falso, (já existem até websites especializados na oferta de uma ampla selecção de fotos de terceiros, de acordo com diferentes perfis, para esta finalidade); ou, o utilizador cria o "*fake"* a partir de uma pessoa real, viva ou morta, utilizando o nome, a fotografia, e uma série de outros elementos.

Neste último caso, o responsável poderá incorrer em diversos crimes (ver página 16), já que o uso indevido de dados pessoais e intransmissíveis sem o consentimento da pessoa, acarreta uma série de riscos.

Que problemas/riscos estão relacionados com o uso de perfis falsos?

A violação de direitos fundamentais como o direito à reserva da intimidade da vida privada, o direito à honra e ao bom nome, o direito à imagem, são problemas que resultam da série de exemplos supra referidos, os quais evidenciam riscos concretos como coacção, difamação, etc. Mas não são os únicos. Desde a perda de controlo dos dados à dificuldade em apagá-los; a apropriação ilegítima de identidades; ou mesmo a quase ausência de moderação por parte das entidades gestoras dos *websites*, todas estas situações se revelam preocupantes em sede de criação de perfis falsos.

E, embora esta técnica não seja específica das redes sociais, quando utilizada nestes meios torna-a mais visível e aumenta o risco de propagação de problemas. E porquê? Em primeira linha porque o acesso à informação e a imagens de terceiros é muito facilitado, basta copiar as imagens colocadas num perfil e divulgá-las, distorcê-las e até inseri-las noutras situações,

[8] Exemplo em http://www.bbc.co.uk/portuguese/noticias/2011/07/110726_twitter_perfil_espanhola_ex_namorado_mm.shtml. Acesso a 30 de Abril de 2012.

descontextualizando-as completamente. Em segundo lugar, porque é muito fácil um utilizador perder o controlo dos dados que coloca na sua página pessoal, já que quando algo é colocado *online* pode ser facilmente copiado e distribuído e, como se não bastasse, torna-se extremamente difícil eliminar os dados por completo, mesmo depois de apagados. Mais, o acesso aos dados pode mesmo efectuar-se através de ataques de *phishing*[9] sob entidade falsa. Por outro lado, os utilizadores assumem que aquele perfil é verdadeiro, bem como a informação que dele consta e, sem questionarem, começam a partilhar todo o tipo de conteúdos com o criador do "fake", o que lhe facilita ainda mais a vida. Também se pode dar o caso de a pessoa alvo não ter um perfil na rede social em causa (exemplo do perfil da professora), logo mais dificilmente terá conhecimento do mesmo, pelo que o controlo da situação se tornará muito mais difícil. E ainda, o facto de o acto ser normalmente dirigido a um público restrito, que lhe dará mais importância, contribui para o propósito do criador do perfil (o que se pode evidenciar no caso da criação de um perfil falso de um político, por exemplo). Todas estas situações conduzem a um perigo maior: a apropriação ilegítima de identidades *online*, um crime já tipificado em alguns ordenamentos jurídicos.

Também a quase ausência de moderação por parte das entidades que administram os *websites* das Redes Sociais se torna um problema, uma vez que embora estas empresas tenham pessoas especializadas encarregues de monitorizar os conteúdos das páginas pessoais, os sítios Web das redes sociais virtuais possuem demasiados utilizadores para o número de moderadores existentes, o que facilita a inserção e manutenção de conteúdos que vão contra as regras de funcionamento dos sites.

Em suma, há que ter especial atenção a toda esta problemática, já que "não é possível apagar o nosso passado na Internet e tudo o que fazemos *online* fica à distância de um clique"[10], isto é, as nossas contas são desactivadas em vez de apagadas, os nossos dados pessoais podem facilmente ser recolhidos, armazenados ou mesmo vendidos por empresas como o *Facebook*, *Google*, ou qualquer um dos inúmeros *websites* onde os utilizadores publicam fotografias e fornecem dados particulares, podendo por sua vez ser usados por Bancos, companhias de seguros, ou para efeitos de marketing.

---

[9] *Phishing* é uma forma de fraude eletrónica, caracterizada por tentativas de adquirir fotos e músicas e outros dados pessoais, ao se fazer passar como uma pessoa confiável ou uma empresa enviando uma comunicação eletrônica oficial.

[10]http://www.new4media.net/pt/?det=10559&id=2434&mid=11. Acesso a 30 de Abril

b) Perfis Mortos

Outra problemática associada à nova era digital é a criação de "cemitérios virtuais". O fenómeno teve origem na rede social *Orkut*: os falecidos que tinham o perfil já formulado permaneceram activos na rede, o que motivou os utilizadores a visitar o perfil e a utilizá-lo como uma espécie de cemitério virtual, deixando mensagens de cunho religioso, manifestando saudades e os pêsames pela perda da pessoa. O perfil da pessoa morta transforma-se, assim, num memorial, onde as pessoas colocam fotos e textos do parente falecido; acedem às suas informações sobre gostos pessoais ou às últimas mensagens enviadas; promovem discussões filosóficas e religiosas; investigam a causa da morte; divulgam informações sobre missas, ou divulgam campanhas publicitárias (por exemplo contra o álcool); criam fundações para receber doações por causas defendidas pelo falecido. Em suma, o perfil é usado como uma forma de expressar a dor e o sofrimento pela perda do falecido, um ritual simbólico de despedida que pode vir a demonstrar-se muito importante no processo de elaboração do luto, dizem os psicólogos entendidos. Todavia, se estas são as pequenas vantagens associadas, maiores são as desvantagens: o processo de remoção do perfil pode acarretar um desgaste emocional muito grande para os familiares; o manter o perfil de alguém próximo activo pode ter o significado de factor de negação da morte e, acima de tudo, significar um desrespeito para com a memória do falecido; mais, a pessoa falecida continua online como se ainda fosse viva, e os seus amigos e familiares, cada vez que abrem o seu perfil, vêm a pessoa querida, continuam a receber convites da mesma, etc.

É um problema real saber o que acontecerá com a nossa vida *online*. A melhor opção a tomar será apagar a página do *website*, contudo, só o representante legal o pode fazer, uma vez que é requisito da remoção do perfil o *upload* da certidão de óbito. Não seria então mais fácil o próprio sistema excluir automaticamente o perfil após um determinado período de inactividade?

Como resolver todas estas situações?

Torna-se urgente encontrar soluções para minimizar os riscos supra mencionados. Em primeira linha, e quanto à dificuldade de controlo das entidades gestoras dos *websites* das redes sociais, é esperado que os utilizadores se monitorizem uns aos outros, reportando aos moderadores a existência de conteúdos inapropriados nos perfis visitados. Todavia, mesmo quando há denúncia desses conteúdos e os mesmos são retirados, é difícil vigiar esse perfil e ver se estes são novamente colocados *online*. Quando uma conta é cancelada, torna-se igualmente complicado barrar o acesso

desse utilizador a um *website* gratuito – nada o impede, portanto, de abrir nova conta e inserir dados diferentes, usufruindo impunemente da sua nova conta. E isto porque quando tal acontece, a entidade não fornece os registos electrónicos que ajudariam a identificar a autoria do ilícito, o que estimula a impunidade e os incidentes acabam por se repetir posteriormente.

É então de extrema importância que o utilizador conheça as formas de se proteger contra possíveis ameaças. Quanto a este propósito, um estudo[11] divulgado por uma multinacional dedicada à segurança na internet analisou quase 3 mil perfis e evidenciou quais as principais diferenças entre perfis falsos e perfis reais, sendo que: quase 60% dos perfis falsos alegam ser bissexuais, mais 10 vezes que os reais; os falsos têm seis vezes mais amigos que os reais: uma média de 726 contra 130; 97% dos perfis falsos alegam ser mulheres, contra 40% dos reais; 43% dos falsos utilizadores nunca actualizam o seu estado; 68% dos falsos diz ter estudos superiores, contra 40% dos reais.

Mas esta não é a única forma de os utilizadores se protegerem. O recomendável passa por accionar a justiça para se tomarem medidas preventivas de preservação das provas. E, claro, exigir indemnização cível pelos danos causados.

Outra solução que se mostra adequada, especificamente quanto à criação de perfis falsos e de perfis de pessoas mortas, é o denominado direito ao esquecimento.

i) Direito ao esquecimento – "Right to be forgotten"

O direito ao esquecimento/desaparecimento propõe-se ser um direito de defesa dos cidadãos, um direito de controlo dos seus dados pessoais, que lhes permitirá controlar a disponibilização *online* dos mesmos, independentemente de ter sido autorizada. Permitirá, assim, exigir a empresas como o Facebook que apaguem todos os seus dados pessoais ao cancelarem o serviço, o que passa pela remoção de todos os dados de páginas da Internet onde se encontrem incluídos, e pela eliminação de quaisquer referências aos mesmos feitas pelos motores de busca. Este direito teve origem no caso Max Schrems[12]. Neste caso, um estudante processou o Facebook por guardar informações suas sem o seu consentimento e que já haviam sido, supostamente, por si apagadas. O jovem concluiu que todo o conteúdo *online* referente a si não tinha sido apagado, mas simplesmente armazenado nos servidores da rede social.

---

[11] http://visao.sapo.pt/pistas-para-identificar-perfis-falsos-no-facebook=f645723#ixzz1rjIPhX8c. Acesso a 30 de Abril de 2012.
[12] http://www.youtube.com/watch?v=ObbiBeXevkE. Acesso a 30 de Abril de 2012.

Este sucedido motivou a Comissão Europeia a propor uma reforma[13] global das regras de proteção de dados para reforçar o controlo exercido pelos utilizadores sobre os seus dados, incluindo o direito ao desaparecimento na rede – o «direito ao esquecimento», nos termos do artigo 17.º da Proposta de regulamento do Parlamento Europeu e do Conselho relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a protecção de dados). Disse a Comissária Europeia encarregada da Justiça e dos Direitos Fundamentais, Viviane Reding, que "a proteção dos dados pessoais é um direito fundamental de todos os europeus, mas os cidadãos nem sempre sentem que controlam plenamente os dados que lhes dizem respeito", esses dados são usados por "todas as empresas do mundo: desde companhias de seguros a bancos ou páginas de redes sociais e ferramentas de busca" como o *Google*. Os objectivos a que se propõe a CE são, de entre outros: a criação do "Direito a ser esquecido" – direito a apagar definitivamente fotografias e comentários, "desde que não existam motivos legítimos para a sua conservação"; imposição de limites em relação ao tempo que os sites e redes sociais podem armazenar a informação dos utilizadores, tal como a quantidade de dados que são visíveis online depois de ter sido requerida a sua remoção; direito a processar os sites em caso de incumprimento da ordem do utilizador; direito à portabilidade dos dados – mais facilidade de acesso aos seus próprios dados e possibilidade de os transferir de um prestador de serviços para outro; dever das empresas de notificarem à autoridade nacional de controlo as violações graves em matéria de dados o mais rapidamente possível (se possível, no prazo de 24 horas); aplicação, pelas autoridades nacionais, de coimas (até 1 milhão de euros ou até 2% do volume de negócios anual global de uma empresa) às empresas que violem as regras em matéria de proteção de dados na UE.

O *Facebook* contudo opõe-se ao "esquecimento", invocando que retirar o material da internet se torna complicado, uma vez que quando algo é colocado *online* pode facilmente ser copiado e distribuído, pelo que destruir o original não será a solução para impedir as pessoas de encontrarem uma cópia noutro lado. Defendem os especialistas que a solução para uma total protecção da privacidade passa por não colocar, de todo, informação *online*.

Mas será que os utilizadores se devem resignar a esta desprotecção? Não existirão alternativas para proteger os nossos dados? Os dados pessoais, mesmo depois de serem tornados públicos, não deixam de ser pessoais, pelo que os titulares não podem ser privados da protecção a

[13] http://www.tvi24.iol.pt/tecnologia/internet-dados-pessoais-redes-sociais-facebook-twitter-tvi24/1320102-4069.html. Acesso a 30 de Abril de 2012.

que têm direito no que toca ao tratamento dos seus dados, direito este consagrado constitucionalmente no artigo 35.º[14].

c) As Crianças nas Redes Sociais

Tendo em conta o incremento do número de crianças que frequentam as redes sociais será importante reflectir sobre três aspectos: a vulnerabilidade das crianças; as predefinições de privacidade; e os incentivos no âmbito da UE.

As crianças estão expostas ao mesmo tipo de riscos a que estão os adultos, só que com maior vulnerabilidade. Segundo o estudo do projecto "*EU Kids Online*" [15] na ordenação dos riscos experimentados a transmissão de informação pessoal surge como o comportamento de risco mais recorrente, enquanto que o encontro real com um contacto conhecido através da internet é muito menos comum, mas permancece como o risco mais perigoso. Existem dois riscos relacionados com esta vulnerabilidade que são bastante importantes por serem muitas vezes experienciadas por crianças: o "cyberbullying" e o "cyberstalking". São importantes porque as atitudes dos autores de "cyberbullying" ou de "cyberstalking" podem eventualmente configurar alguns ilícitos, tais como: crimes contra a honra, o crime de ameaça ou de coacção. No entanto, note-se que sendo os autores do "cyberbullying" menores de 16 anos, há uma inimputabilidade penal dos mesmos (art.19.º do Código Penal). Como estas práticas podem traduzir-se num crime, será importante, se for o caso de uma prática agravada, não ceder à tentação de apagar os comentários feitos pelo infractor na rede social, pois os mesmos poderão servir como meio de prova. Tendo em conta que existe a possibilidade do autor que publica o conteúdo, posteriormente, o remover, pertinente será fazer uma pequena nota a propósito da conservação da prova. Vislumbram-se quatro opções neste tipo de casos: a) a autoridade judicial faz uma injunção à empresa que administra o website: esta empresa fica então obrigada a bloquear a página, para que se conserve a prova; b) recurso à prova testemunhal: testemunha depõe como viu que o perfil tinha os comentários dos quais dependem o preenchimento do tipo objecto do crime em causa; c) o utilizador faz um "*printscreen*" sobre a

---

[14] Artigo 35.º CRP - Utilização da Informática: 1 - *Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes dizem respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.*

[15] Press release 11/479 de 18 de Abril de 2011 da Comissão Europeia. http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/479&format=HTML&aged=0&language=PT&guiLanguage=en. Acesso a 18 de Abril de 2012. Para um resumo do projecto: http://www.fcsh.unl.pt/eukidsonline/docs/SumarioEUKOL1.pdf .Para mais informações: www.eukidsonline.net

página (documento sobre um documento); d) Já dentro de um processo aberto, uma medida de coacção de proibição de contactos (200.º al.d) do CPP).

Quanto aos parâmetros de privacidade: apenas 56% dos jovens dos 11 aos 12 anos declaram saber como mudar os parâmetros de privacidade no seu perfil registado em redes[16]. Neste caso, é notório que, para as crianças, as definições de privacidade por defeito, ou seja, as configurações iniciais de privacidade *standart*, assumem uma grande importância. Uma vez que um grande número destas crianças não sabe ou não alterou as suas definições de privacidade, as configurações que têm são as definições de privacidade por defeito. Nesta sede seria crucial impor às empresas que detêm e administram os websites de redes sociais que estabelecessem uma pré-configuração mais protectora da privacidade dos utilizadores. E, uma vez que a fiscalização da idade dos utilizadores não é feita pelas empresas, esta pré-configuração teria de servir para todos os utilizadores, para que não se criasse um risco de não se abranger a totalidade das crianças.

Uma questão crucial será: Como é que podemos lidar com os riscos a que estão sujeitos as crianças?

Em primeiro lugar, consideramos que a mediação parental é importantíssima. Para além da mediação parental, será bastante importante um equilíbrio entre a capacitação e a protecção: isto porque se aumentarmos o acesso e o uso da internet, então, também estamos a aumentar os riscos *online*; por outro lado, as estratégias para diminuir os riscos podem restringir as oportunidades *online* das crianças, podendo assim prejudicar os seus direitos ou limitar a sua aprendizagem. O equilíbrio destes dois pontos poderia ser conseguido com o incentivo da literacia digital e com regulamentação, ou seja, com auto-regulação e com hetero-regulação. Quanto à literacia digital, actualmente há uma presença insuficiente ou desactualizada das TIC nas escolas, que deve ser rapidamente resolvida. Com este obstáculo ultrapassado as crianças poderiam desenvolver uma consciência sobre a realidade virtual. Se estas estiverem mais de alerta para os riscos vão, deste modo, conseguir reduzir e controlar alguns dos impactos negativos da web. Quanto à regulação, a Comissão está a ser activa nesta área. Em 2009, fez um acordo de auto-regulação assinado pelas empresas de redes sociais através do qual estas se comprometeram a aplicar uma série de medidas de modo a garantir a segurança dos menores. Este acordo foi denominado de "*Safer Social Networking Principles*".[17] Os

[16] Press release 11/479 de 18 de Abril de 2011 da Comissão Europeia.

[17] "Safer Social Networking Principles for the EU". http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf. Acesso a 26 de Abril de 2012.

princípios são os seguintes: aumentar a consciencialização com mensagens educativas de segurança e políticas de uso aceitáveis para os utilizadores, pais, professores e encarregados de educação de uma maneira clara e apropriada para a idade; trabalhar para garantir que os serviços são apropriados para a idade consoante o público-alvo; capacitar os utilizadores através de ferramentas e tecnologia; fornecer mecanismos fáceis de usar para relatar condutas ou conteúdos que violem os Termos de Serviço; responder a notificações de conteúdo ou condutas ilegais; habilitar e incentivar os utilizadores a utilizar uma abordagem segura quanto às suas informações pessoais e privacidade; e, avaliar os meios que fazem a revisão do conteúdo/conduta ilegal ou proibido. No entanto, em Julho de 2011[18] e em Setembro de 2011[19] a Comissão revelou que a maioria das empresas não cumpre este acordo, ou seja, seria crucial impor mais firmemente às empresas, que detêm e administram os websites de redes sociais, que estabelecessem uma pré-configuração mais protectora da privacidade, especialmente das crianças devido ao facto de estas por vezes não saberem o que é um parâmetro de privacidade, nem muito menos saberem como o alterarem.

d) Despedimentos relacionados com a revelação de dados pessoais e íntimos nas redes sociais

Existem dois tipos de situações que podem levar as empresas a sancionar um empregado devido às redes sociais: o seu uso, por criar "dependência que leva à perda de produtividade", e a publicação de comentários sobre colegas, empresa ou entidade patronal. Se no primeiro caso as consequências podem não passar de uma repreensão ou processo disciplinar, no segundo, e dependendo da gravidade, o desfecho pode ser o despedimento com justa causa. Em Portugal já foi relatado, pelo menos um caso de um despedimento relacionado com a utilização de redes sociais[20], e, um pouco por todo o mundo têm sido noticiados casos de despedimentos com estes contornos. Estes casos são bastante controversos porque não há uma legislação sobre a forma como as empresas se devem relacionar com as redes sociais, no entanto, tudo o que se passa nas redes sociais não fica à margem da lei.

Nestes casos de despedimento, existem diferentes interesses conflituantes: os direitos fundamentais do trabalhador, como sendo o direito à liberdade de expressão e de opinião e o direito à

[18] Comunicado de Imprensa. IP/11/762 http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/762&format=HTML&aged=1&language=PT&guiLanguage=en. Acesso a 26 de Abril de 2012.
[19] Dailymotion, Google, Microsoft Europa, Skyrock, Netzwerke, Stardoll, Sulake, Yahoo Europa e Wer-kennt-wen
[20] http://www.sabado.pt/Multimedia/FOTOS/-span--b-Sociedade-b---span--(1)/Fotogaleria-(7).aspx. Acesso a 30 de Abril de 2012.

reserva de intimidade da vida privada; e os deveres do trabalhador para com o empregador: dever de lealdade e de urbanidade.

Relativamente à liberdade de expressão (art.37.º CRP e 14.º do Código do Trabalho), esta pode ser manifestada a propósito de questões conexas com o trabalho. No entanto, existem dois limites ao exercício desta liberdade: o respeito pelos direitos de personalidade da outra parte e, o normal funcionamento da empresa. Por exemplo, não é admissível ao trabalhador de uma empresa que efectue perante clientes críticas à gestão da empresa, uma vez que a reacção natural dos mesmos será a de deixar de adquirir bens ou serviços desta. Na maior parte dos casos de despedimento relacionados com as redes sociais são estes limites que estão em causa.

Quanto a decisões jurisprudenciais sobre este assunto, como exemplo podemos dar as seguintes decisões: 1 - O *Conseil de prud'hommes* - jurisdição de primeira instância competente para julgar litígios de trabalho, em França - considerou fundamentado o despedimento de dois funcionários acusados de terem manchado o nome da empresa através da rede social Facebook. O advogado da empresa fez valer a sua posição, que insistia que uma rede social não deve ser considerada um sítio privado mas antes uma plataforma aberta. E ganhou. O tribunal deu razão aos argumentos apresentados pela empresa[21]; 2 - Também um tribunal holandês deu razão a uma empresa que despediu um funcionário, depois de este ter publicado insultos numa rede social. O ex-funcionário alegou que os comentários eram privados, mas tal não convenceu o juiz, que defendeu que a empresa teve razão ao despedi-lo, ao afirmar que «os argumentos do funcionário de que o Facebook pertence ao domínio privado do empregado são, na opinião deste tribunal, incorrectos», lê-se na sentença citada pela imprensa local. Para o juiz encarregue de analisar o caso tal deve-se ao facto de todos os comentários e mensagens publicadas poderem ser republicadas facilmente, tal como aconteceu no caso, o que faz com que a informação seja visível para outras pessoas e seja considerada semi-pública[22]; 3 - Já no Reino Unido, um funcionário também viu um tribunal confirmar o seu despedimento. De acordo com o tribunal, embora os comentários tenham sido feito fora da hora de expediente e na página privada do funcionário, o mesmo não é garante de privacidade e as opiniões

[21] http://www.tvi24.iol.pt/tecnologia/facebook-despedimentos-franca-comentarios-rede-social-tvi24/1210694-4069.html. Acesso a 30 de Abril de 2012.
[22] http://sol.sapo.pt/inicio/Tecnologia/Interior.aspx?content_id=44982. Acesso a 30 de Abril de 2012.

expressas podem ser utilizadas pelos seus «amigos» na rede social, que poderão espalhá-las por um vasto número de pessoas[23].

Será importante referir que a colocação de comentários podem pôr em causa o bom nome da empresa ou dos colegas, mas que, no entanto, o despedimento por justa causa só será possível se estiver comprometida a continuidade da relação laboral.

3. Revelação de dados pessoais e íntimos nas redes sociais: responsabilidade e implicações a nível do Direito Penal

Se é um facto que a sociedade em rede possibilitou ao indivíduo uma maior exposição, facilidade de intercomunicação e de divulgação, todavia permitiu também que novos ilícitos fossem praticados, causando por vezes prejuízos incalculáveis, já que a extensão do dano pode ser muito maior quando praticada via Internet.

Surge então um verdadeiro problema: quem responsabilizar pelos conteúdos colocados *online*? Se é o próprio utilizador a colocar informação na rede social, então é por sua conta e risco que deve correr o risco da perda de controlo dos dados que expõe. Todavia, a situação agrava-se quando a informação é colocada por terceiros (sejam amigos ou desconhecidos). Aqui, entram em colisão direitos fundamentais: se por um lado temos direito à privacidade e à protecção dos dados pessoais, por outro lado, quem publicou o comentário/imagem tem direito à liberdade de expressão e à livre manifestação do pensamento *online* e os terceiros utilizadores direito à informação. Mas se escrevemos "ontem à noite o utilizador X estava bêbedo", trata-se do nosso direito à liberdade de expressão, mas também de informação pessoal do utilizador X, pelo que há que fazer uma justa ponderação destes direitos, e optar pela prevalência daqueles que se revelem superiores consoante o caso em concreto, tal como se depreende do artigo 18.º, nº2 da CRP.

Então, a criação de um perfil falso na internet é um ilícito?

Criar um perfil falso de alguém que não existe, só para preservar a sua identidade durante os relacionamentos na internet, sem que esta prática tenha causado qualquer dano, não é crime. Todavia pode levar o criador a ter de remover o seu perfil, ou por infracção dos Termos de Uso estipulados

[23] http://sol.sapo.pt/inicio/Tecnologia/Interior.aspx?content_id=32849. Acesso a 30 de Abril de 2012.

pelo website, ou caso exista alguma denúncia e, aí, poderá ter de suportar uma indemnização, no caso de existirem meios de prova que comprovem a violação dos direitos de imagem. Já se o "fake" for criado através de uma pessoa real, o facto de utilizar a imagem e a personalidade de outra pessoa, escrever declarações falsas com fim de a prejudicar, ou alterar a verdade sobre determinado facto juridicamente relevante, pode levar o responsável a incorrer no crime de roubo de identidade online – um crime ainda não tipificado em Portugal, mas que já o é em Nova Iorque e na Califórnia, por exemplo. Mais, se o utilizador criar um perfil falso meramente a título de brincadeira (como tantos jovens o fazem hoje em dia), mas se ultrapassar os limites legalmente estabelecidos, então poderá praticar crimes contra a honra, tais como calúnia, difamação, injúria.

Em género de conclusão, o responsável pela criação de um perfil falso, bem como qualquer utilizador que infrinja regras legalmente estabelecidas para a criminalidade informática pode vir a ser civilmente responsabilizado, por danos morais e patrimoniais eventualmente causados, mas também o pode ser penalmente, por uma série de crimes abaixo indicados na Tabela (para melhor visualização e compreensão) e que se reportam às variadas situações mencionadas anteriormente.

Conduta	Crime	Legis Lação	Pena
Mencionar numa rede social que alguém se deve matar ou sugerir como fazê-lo (se o suicídio vier efectivamente a ser tentado ou consumado)	Incitamento ao suicídio	135.º CP	Pena de prisão até três anos. Se a pessoa incitada for menor de 16 anos ou tiver a sua capacidade de valoração ou de determinação sensivelmente diminuída: pena de prisão de um a cinco anos.
Mencionar características negativas de uma pessoa (gordo, feio, ignorante…) num chat de uma rede social	Injúria	180.º CP	Pena de prisão até 6 meses ou com pena de multa até 240 dias.
Mencionar numa rede social que alguém cometeu algum crime	Calúnia	183.º CP	Pena de prisão até 2 anos ou com pena de multa não inferior a 120 dias.
Enviar uma mensagem em que diz que vai matar a pessoa ou causar-lhe algum mal	Ameaça	153.º CP	Pena de prisão até um ano ou com pena de multa até 120 dias.
Divulgar factos relativos à vida privada de outrem numa rede social	Devassa vida privada	192.º CP	Pena de prisão até 1 ano ou com pena de multa até 240 dias.

Tabela 1 – Responsabilidade penal de certas condutas de utilizadores de redes sociais

Para além destas situações, na Internet proliferam outras atividades susceptíveis de violar o direito à reserva da vida privada, e que consubstanciam o Cibercrime, tais como: a apropriação

ilegítima de identidades; o aproveitamento de nomes de figuras públicas para criação de domínios (art. 193.º CP); a divulgação, sem autorização, de imagens, correspondência ou outros dados de terceiros (art. 193.º e 199.º CP); a disseminação de vírus ou *software* de espionagem (*spyware*) (art. 4.º, nº1 Lei 109/09). Mas também as empresas que omitem a remoção de conteúdos ilícitos devem ser responsabilizadas. Assim foi o caso do Google[24] que foi recentemente processado no pagamento de uma indenização de 30 mil reais por danos morais causados a uma a usuária. A decisão ocorreu no Tribunal de Justiça do Rio de Janeiro, numa situação em que alguém criou no Orkut um perfil falso de uma mulher que se dizia "na idade da loba, faminta por sexo, totalmente liberal, sem preconceitos", entre outras coisas, o criador do perfil ainda incluiu o telefone e o endereço dela. Nos casos de danos causados pela incidência de perfis falsos no Orkut, o Google é processado por fornecer suporte tecnológico e favorecer a prática do ilícito.

Neste sentido, os EUA sistematizaram a responsabilidade civil dos gestores de serviços de Internet com a aprovação do *Communications Decency Act* (CDA) e do *Digital Millenium Copyright Act* (DMCA), leis que estipulam as circunstâncias em que os administradores poderão ser responsabilizados pelos actos praticados pelos seus utilizadores, e que se guiam pelo princípio do "*notice and takedown*", que consiste na responsabilidade de remover o conteúdo do ar, assim que tomar conhecimento da sua ilicitude. Raciocínio em sentido inverso foi adoptado pela Comunidade Europeia que publicou a Directiva 2000/31, a qual isenta os administradores de responsabilidade sobre o controle prévio do conteúdo, salvo quando são devidamente notificados da prática ilícita.

4. Revelação de dados pessoais e íntimos nas redes sociais: existe privacidade?

Como já foi referido as redes sociais virtuais são grupos ou espaços específicos na Internet, que permitem partilhar dados e informações, sendo estas de caráter geral ou específico, das mais diversas formas (textos, arquivos, imagens fotos, vídeos, etc.). Acontece que muitas das vezes os utilizadores destas redes expõem grande parte do que é a sua vida privada neste tipo de *site*. O que nos leva à seguinte questão: o que partilhamos nas redes sociais está inserido na esfera pública ou na esfera privada? A resposta a esta questão é bastante importante, especialmente nos casos de despedimento referidos supra. Como já foi dito, parece que a jurisprudência tende a considerar que as redes sociais na Internet são plataformas abertas, consequentemente, ligadas à esfera pública.

[24] http://g1.globo.com/Noticias/Tecnologia/0,,MUL1299274-6174,00-GOGLE+E+MULTADO+EM+R+MIL+POR+PERFIL+FALSO+DE+FAMINTA+POR+SEXO+NO+ORKUT.html. Acesso a 30 de Abril de 2012.

Numa concepção clássica, a teoria das três esferas, com origem na vasta literatura alemã ("Sphärentheorie"), revestiu-se de um papel fundamental na construção e delimitação do âmbito de protecção do direito à reserva da intimidade da vida privada.

De acordo com esta teoria, existem três esferas: 1- A e*sfera da vida íntima ou da intimidade*, que corresponde a um domínio inviolável e intangível da vida privada, subtraído ao conhecimento de outrem; informações de tal forma reservadas que, em regra, nunca serão acessíveis a outros indivíduos. Dentro desta esfera podemos encontrar aspectos relativos à vida sentimental, estado de saúde ou de gravidez, vida sexual, convicções políticas e religiosas, etc; 2 – A *esfera da vida privada*, que abrange factos que cada um partilha com um núcleo limitado de pessoas, ou seja, encontramo-nos num plano menos inacessível, mas igualmente reservado, que pode variar de pessoa para pessoa, uma vez que engloba os hábitos de vida e as informações que o indivíduo partilha com a sua família e amigos, e cujo conhecimento o respectivo titular tem interesse em guardar para si; 3 – A *esfera da vida pública*, que envolve factos susceptíveis de serem conhecidos por todos. Respeita à participação de cada um na vida da colectividade e contempla os comportamentos e atitudes deliberadamente acessíveis ao público e susceptíveis de serem conhecidos por todos, em relação à qual não existe qualquer tipo de reserva.

Em que esfera se inserem então estas práticas? Conseguimos deslumbrar dois critérios possíveis: ou adoptamos o critério da esfera pública, e defendemos que a partir do momento em que um indivíduo cria um perfil social, está susceptível à exposição de factos quotidianos e de comportamentos, para além dos expostos pelo próprio. Ou seja, também os seus "amigos" da rede podem expor a vida do utilizador, seja através das identificações, os chamados "tags", seja através de publicações no mural ou até de partilha de fotos e vídeos. Isto diminui consideravelmente o seu carácter privativo. Diminui-o de tal modo que a esfera passa a ser pública. É muito fácil um utilizador perder o controlo dos dados que coloca na sua página pessoal: assim que um dado fica online, muito dificilmente desaparecerá, mesmo se depois for apagado. Ou seja, um facto que, à partida, seria enquadrável na esfera privada ou na esfera íntima, a partir do momento em que é partilhado numa rede social, passa a ser enquadrável no âmbito da esfera pública do indivíduo, devido à potencialidade que este conteúdo tem de ser partilhado. A rede social é uma plataforma aberta, logo, por ser de acesso generalizado, isto significa que são factos susceptíveis de serem conhecidos por todos. Note-se que este critério não é sensível ao tipo de definição de privacidade que o utilizador dá aos conteúdos que publica no seu perfil numa rede social. Resumindo: tudo o que for colocado na Internet deixa de ser privado e as redes sociais não serão excepção. Mesmo que o perfil

esteja definido como privado, nada impede a quem tenha acesso autorizado ao mesmo de copiar os conteúdos e enviá-los a terceiros; Ou então adoptamos um critério personalizável. Este critério é por nós denominado de "critério personalizável", porque o critério será distinto consoante o usuário e a configuração de privacidade do conteúdo publicado. Quer com isto dizer-se que um conteúdo definido como privado (só visível para "amigos") estará ainda dentro da esfera privada, já, contrariamente, um conteúdo marcado como público (visível online, independentemente de se ter ou não um perfil naquela rede social), será enquadrável na esfera pública do utilizador.

Ainda relativamente à lógica deste último critério apresentado, pode colocar-se um outro problema: quando há uma alteração das definições privacidade, ou seja, quando um utilizador altera um conteúdo de público para privado, ou de privado para público, altera-se a "esfera" com esta alteração? A resposta, mais uma vez, também dependerá. Dependerá do tipo de alteração. Porque, se o conteúdo passar de privado para público: há uma alteração efectiva do carácter privativo do conteúdo, ou seja, o conteúdo deixa de ser privado para ser público devido a esta alteração do utilizador. No entanto, se a modificação consistir numa alteração de um conteúdo público para um conteúdo privado, já não podemos aceitar que o conteúdo deixa de estar enquadrado na esfera pública para estar na esfera privada. Isto porque, uma vez definido como público não pode entrar de novo na esfera privada do utilizador.

Um novo conceito de "amigos"

Ao abrir-se uma conta numa rede social aceita-se "a priori" que parte da vida privada vai ser exposta, pelo menos ao nossos supostos "amigos". No entanto, por mais íntimos que alguns desses "amigos" sejam, há sempre uns que nunca o serão verdadeiramente.

Na concepção clássica da teoria das três esferas, a esfera privada cinge-se às informações que o indivíduo partilha com a sua família e amigos mais próximos; já a esfera pública é definida como sendo os factos susceptíveis de serem conhecidos por todos. Consequentemente, um perfil privado de uma rede social, não se enquadra nem totalmente na esfera da vida privada, nem na esfera pública.

O que temos é um novo conceito de amigos que engloba: amigos mais próximos, conhecidos e, por vezes, para quem não faz uma verificação das identidades de quem está a adicionar na sua rede ou para quem a popularidade se define pelo número de amigos adicionado na rede, e que aceita praticamente todos os pedidos de amizade que lhe são feitos, desconhecidos.

O que nos pode levar a adoptar uma nova esfera: uma esfera que se situa entre a esfera privada e a esfera pública, uma esfera semi-pública, como refere o Tribunal holandês no caso de despedimento referido supra, para contemplar esta nova realidade. Esta nova concepção seria necessária pela falta de resposta dada nas concepções clássicas. Esta insuficiência compreende-se porque, embora sempre tivessem existido redes sociais, estas nunca foram pensadas num âmbito de uma plataforma como a internet. A questão fulcral neste tipo de concepção será de saber que tipo de protecção merece esta esfera. A regulação das redes sociais, pode passar por definir se existe ou não privacidade, ou seja, que tipo de protecção tem esta esfera semi-pública.

5. Será necessária a intervenção do legislador ordinário ou bastará a elaboração de códigos de conduta?

Observados os problemas suscitados por este recente fenómeno torna-se imperioso desenvolver modos de lidar com estes. A regulação das redes sociais é a solução apontada, mas será necessária a intervenção do legislador ordinário (hetero-regulação) ou bastará a elaboração de códigos de conduta (auto-regulação)? Esta é a questão a que vamos atender.

a. A via da auto regulação – os códigos de conduta

Esta seria a via mais branda de lidar com as questões suscitadas. Não significa isto, no entanto, que a via peque por falta de eficácia.

A consciência social quando liga com novas realidades tende a desenvolver , naturalmente, códigos de conduta. Ao longo do tempo vão se criando hábitos que acabam por se implantar e criar uma convicção de obrigatoriedade. No entanto, este processo tende a ser evolutivo e portanto algo demorado. Ora, estas novas realidades sociais no campo virtual desenvolveram-se a um ritmo acelerado e não permitiram que fossem assimiladas devidamente as regras de conduta nestas situações. Os utilizadores lidaram com este fenómeno sem prever as nefastas consequências que daí podiam resultar. Tornou-se agora aparente a necessidade de criarmos parâmetros de actuação nas redes socias para que estes sejam ensinados a todos os que as frequentam ou irão frequentar. Surge assim a auto-regulação.

Do que se trata afinal a auto-regulação? Esta passaria pela elaboração de códigos que regulem a conduta dos utilizadores nas redes sociais. Estes são conjuntos de regras que orientam e disciplinam a conduta de um determinado grupo de pessoas, de acordo com os princípios postulados

no código e que visam proteger, os utilizadores, dos efeitos prejudiciais que as suas condutas podem ter nestes meios.

Estes códigos de conduta seriam elaborados pelas próprias redes sociais ou pelos seus utilizadores de acordo com as necessidades sentidas, por isso apresentam a vantagem de estarem harmonizadas com o objecto que regulam pois estão directamente relacionadas. As soluções que apresentam tendem a ser mais adequadas às necessidades e interesses em causa.[25]

Recentemente, a frequência de conflitos laborais, suscitados por estas redes, levou algumas empresas a definirem políticas de actuação dos seus colaboradores nestas redes para garantir a protecção da empresa. As consequências que podem advir da violação de tais regras podem passar por advertências, processos disciplinares ou até despedimentos por justa causa.

Se não podemos questionar a utilidade destes códigos na prevenção de conflitos laborais ou até na protecção pessoal do utilizador, podemos, no entanto, pôr em causa a legitimidade das empresas para restringir a liberdade de expressão e de opinião dos seus colaboradores se considerarmos que estas redes são espaços privados de partilha. Se considerarmos este espaço de partilha público estes códigos são guias de conduta essenciais para prevenir conflitos pois os trabalhadores podem ser responsabilizados pelas suas afirmações nestes espaços, que coloquem em causa os seus deveres enquanto trabalhador.

Questão diferente mas essencial, quanto aos códigos de conduta das empresas, é que estes devem ser elaborados em conjunto com os trabalhadores. A criação destas regras, por parte das empresas, não poderá contribuir para o enfraquecimento da posição do trabalhador que se vê restringido nalguns dos seus direitos fundamentais, em razão do seu estatuto de trabalhador. Estas equiparam-se a verdadeiros regulamentos e devem ser elaboradas em conjunto com sindicatos ou outras associações de trabalhadores para evitar que os códigos visem exclusivamente proteger a imagem da empresa à custa do direito de liberdade de expressão e do direito à privacidade do seu colaborador. Tem que haver um equilíbrio entre as partes envolvidas.

Serão os códigos de conduta uma solução necessária? Consideramos que sim. A auto-regulação goza da vantagem, já referida, de estar harmonizada com as necessidades sentidas. O

[25] A importância da auto-regulação foi confirmada pela Comissão que está a acompanhar a criação de um acordo de auto-regulação, pelas redes sociais, através do qual se comprometem a aplicar uma série de medidas nos seus serviços de modo a garantir a segurança dos menores.

contacto directo com o objecto regulado permite uma compreensão dificilmente alcançável por um regulador externo. A eficácia desta via está dependente da aposta no ensino destas regras de etiqueta e padrões de conduta, da sua assimilação e efectiva aplicação. Tudo isto contribuirá para criar um novo Utilizador, o *Utilizador Digitalmente Correcto*, que faz um uso ético, seguro e legal da tecnologia. No entanto, esta não é uma via perfeita. A violação destas regras não apresenta consequências gravosas pelo que o seu acatamento pode não ser total.[26] Quando acatadas, estas regras são eficazes mas apenas no plano preventivo, não prevendo formas de lidar com exposição indevida de dados, ou usurpação de identidades entre outros problemas. A importância de uma actuação preventiva nestes meios sociais online é essencial, pois assim que existe uma revelação de dados na internet é muito difícil recuperar o controlo sobre esses dados pelo que a educação dos utilizadores servirá por si só como um factor de protecção. Esta solução terá que ser sempre complementada por outra solução para que a protecção seja total.

b. A via da hetero-regulação – a legislação

Em Portugal não existe regulação específica das redes socias. A protecção dos utilizadores encontra-se numa "manta de retalhos" legal. Ora, este meio social *online* é um meio muito particular o que dificulta a aplicação dos preceitos legais já existentes e por isso reclama a criação de legislação específica. A União Europeia avança agora com uma nova legislação de protecção de dados, que deverá ser ratificada entre 2014 e 2015, que pretende remediar esta situação, dirigindo-se especificamente às redes sociais. Esta nova lei, entre outras coisas, vai garantir o direito ao esquecimento nas redes sociais. Na Alemanha foi proposto, a propósito da privacidade no local de trabalho, que os candidatos a postos de trabalho não possam ser "investigados" nas redes sociais pelos seus futuros patrões. Nos E.U.A já existem leis dispersas que abordam alguns dos perigos das redes sociais. Por exemplo, no estado do Maryland os trabalhadores não podem ser obrigados a revelar as palavras-passes das suas contas nas redes socias para serem contratados ou manter o seu emprego. Na Califórnia existe uma lei que proíbe o *cyber-bullying* e abrange o assédio praticado em redes sociais. No mesmo Estado foi proposta uma lei que obriga as redes sociais a definir as condições de privacidade máxima por defeito.

Estas experiências legislativas estão bem encaminhadas, apesar do esforço de legislação ter que ser mais profundo e abrangente. Consideramos que o primeiro passo será a tomada de posição

[26] A consequência mais gravosa do desrespeito de regras impostas pelas redes é a expulsão da mesma.

sobre se as redes sociais são ou não um espaço privado. Esta é a questão central que poderá facilitar a aplicação dos preceitos legais já existentes a esta realidade ambígua. A segurança que a legislação pode transmitir ao utilizador não pode ser descurada. Esta é a via que deve complementar e reforçar a acção preventiva dos códigos de conduta.

CONCLUSÕES

As redes sociais trazem consigo diferentes impactos jurídicos. Em Portugal não existe regulação específica destas redes, a tutela dos utilizadores encontra-se numa "manta de retalhos" legal. O que nos leva a questionar se esta protecção é suficiente. Isto porque existem condutas que não estão tipificadas, como por exemplo, o roubo de identidade *online*. Outra questão é a falta de protecção das crianças, o que poderá ser contornado através da imposição, por hetero-regulação, de definições de privacidade por defeito mais protectoras.

É importante não esquecer que tudo o que divulgamos nas redes sociais pode ser eliminado pelo utilizador, mas não é realmente apagado. Efectivamente, os dados não são privados, mesmo que o perfil esteja definido como privado, nada impede a quem tenha acesso autorizado ao mesmo de copiar os seus conteúdos e enviá-los a terceiros. Será importante que o utilizador compreenda que se pensar em colocar algo na sua página pessoal que o deixe com dúvidas, opte por não o colocar de todo. Isto é premente na problemática dos despedimentos, porque, embora não exista, actualmente, jurisprudência portuguesa que resolva esta questão, a tendência internacional é considerar as redes sociais como enquadradas na esfera pública do utilizador, independentemente das suas definições de privacidade.

Neste sentido, é necessário definir se as redes sociais são ou não um espaço privado. Na nossa opinião, e de acordo com a tendência internacional da jurisprudência, entendemos que não. Como tal, e no sentido de oferecer ao utilizador mais garantias e segurança, torna-se urgente e imprescindível o alargamento dos preceitos legais já existentes, por forma a reforçar a acção preventiva dos código de conduta.

BIBLIOGRAFIA

Monografias

CASTRO, Catarina Sarmento "Direito da Informática, Privacidade e Dados Pessoais", Almedina, Lisboa, 2005.

FARINHO, Domingos Miguel Soares, "Intimidade da Vida Privada e Media no Ciberespaço", Almedina, Lisboa, 2006.

Sítios na Internet

Acordo de auto-regulação "Safer Social Networking Principles for the EU". http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf. Acesso a 26 de Abril de 2012.

CAMPANA, Márcia, "Facebook opõe-se ao esquecimento", http://www.new4media.net/pt/?det=10559&id=2434&mid=11, acesso dia 30 de Abril de 2012.

Comunicado de Imprensa IP/11/479 de 18 de Abril de 2011 da Comissão Europeia. "Agenda Digital: crianças com idades cada vez mais baixas utilizam redes sociais e muitas não estão conscientes dos principais riscos para a privacidade, revela inquérito.". http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/479&format=HTML&aged=0&language=PT&guiLanguage=en. Acesso a 18 de Abril de 2012.

Comunicado de Imprensa IP/11/762 de 21 de Junho de 2011. "Agenda Digital: apenas dois sítios de redes sociais protegem de raiz a privacidade dos perfis dos menores." INFANTE, Anelise, "Espanhola é presa por criar perfil falso no Twitter para se vingar do ex-namorado", http://www.bbc.co.uk/portuguese/noticias/2011/07/110726_twitter_perfil_espanhola_ex_namorado_mm.shtml, acesso dia 30 de Abril de 2012.

"Conceito de rede social". http://pt.wikipedia.org/wiki/Rede_social, acesso a 16 de Abril de 2012

"Estudante processa Facebook", http://www.youtube.com/watch?v=ObbiBeXevkE, acesso a 30 de Abril de 2012.

"Estudo da UM's WAVE research into the phenomenal growth of social media is the most robust data set in the world", www.universalmccann.bitecp.com/wave4/Wave4.pdf. Acesso a 16 de Abril de 2012.

"Estudo sobre a adesão às redes sociais na internet", http://siteanalytics.compete.com/facebook.com/,acesso a 16 de Abril de 2012.

"Facebook: Em França dá direito a despedimento com justa causa", http://www.tvi24.iol.pt/tecnologia/facebook-despedimentos-franca-comentarios-rede-social-tvi24/1210694-4069.html. 10 de Novembro de 2010. Acesso a 30 de Abril de 2012.

"Google é multado em R$ 30 mil por perfil falso de 'faminta por sexo' no Orkut", http://g1.globo.com/Noticias/Tecnologia/0,,MUL1299274-6174,00-GOGLE+E+MULTADO+EM+R+MIL+POR+PERFIL+FALSO+DE+FAMINTA+POR+SEXO+NO+ORKUT.html, acesso a 30 de Abril de 2012.

"Pistas para identificar perfis falsos no Facebook", http://visao.sapo.pt/pistas-para-identificar-perfis-falsos-no-facebook=f645723#ixzz1rjIPhX8c, acesso a 30 de Abril de 2012.

SANTOS, Liane, "Bárbara Borges é perseguida por perfil falso no Twitter", http://ego.globo.com/Gente/Noticias/0,,MUL1638305-9798,00-BARBARA+BORGES+E+PERSEGUIDA+POR+PERFIL+FALSO+NO+TWITTER.html, acesso dia 30 de Abril de 2012.

"Tribunal confirma despedimento por criticar empresa no Facebook". http://sol.sapo.pt/inicio/Tecnologia/Interior.aspx?content_id=32849. 4 de Novembro de 2011. Acesso a 30 de Abril de 2012.

"Tribunal dá razão a despedimento com base em insultos no Facebook". http://sol.sapo.pt/inicio/Tecnologia/Interior.aspx?content_id=44982. 26 de Março de 2012. Acesso a 30 de Abril de 2012.

"UE quer assegurar direito a «desaparecer» na internet", http://www.tvi24.iol.pt/tecnologia/internet-dados-pessoais-redes-sociais-facebook-twitter-tvi24/1320102-4069.html, acesso a 30 de Abril de 2012.