

Invisible criminality: the risks of social networks

Criminalidade invisível: os jovens e os riscos das redes sociais

Sónia Cruz*

Francisco Restivo**

AbstrAct

This article addresses digital footprint, and reflects on the need of raising awareness among students, parents and teachers of the impact- more or less positive- that digital footprints, left by each individual in their interactions on the Internet, can have in their future life.

Then, we describe the risks young people who have an *e-life* on social networks, and present guidelines for its prevention. Finally, we reflect on the network *ask.fm*, an open social network that has gained wide acceptance among young Portuguese.

Keywords: digital footprint, social networking risks, prevention.

Resumo

A presente comunicação aborda a questão da pegada digital, reflectindo sobre a necessidade de consciencializar alunos, pais e professores para o impacto mais ou menos positivo que a marca digital, deixada por cada indivíduo nas suas interações na Internet, poderá ter na vida futura de cada um.

De seguida, descrevem-se os riscos que os jovens que têm uma *e-vida* nas redes sociais correm, apresentando-se ainda linhas orientadoras para a sua prevenção. Por fim,

reflecte-se sobre a rede *ask.fm*, uma rede social aberta que tem ganho adeptos entre os jovens portugueses.

Palavras-Chave: pegada digital, riscos nas redes sociais, prevenção.

* Faculdade de Ciências Sociais, Universidade Católica Portuguesa - soniacruz@braga.ucp.pt

** Faculdade de Ciências Sociais, Universidade Católica Portuguesa - LIACC, Universidade do Porto - frestivo@braga.ucp.pt

Introdução

As redes sociais, tal como hoje as entendemos, são um fenómeno moderno, resultado dos fantásticos desenvolvimentos das tecnologias da informação e da comunicação, das comunicações e dos terminais cada vez mais acessíveis e mais poderosos. O seu sucesso baseia-se em agregar uma maioria de utilizadores, pois cada um utilizará aquela onde a maioria dos seus amigos se encontra, partilhando comentários e fotos, jogando, criando e divulgando eventos sociais e tudo o que muitos de nós começam a conhecer.

Em menos de dez anos, passámos da percepção da ideia de uma *Web 2.0*, uma *Web* em que todos podíamos aspirar a ser produtores de informação, para a vivência numa sociedade global, sem distâncias, largamente desmaterializada, em que cada um pode viver e competir, criar uma identidade, relacionar-se, produzir, mostrar, vender e comprar, com facilidade sem precedentes (Kaplan, 2010).

Este mundo novo, para uns perfeitamente óbvio, para outros absolutamente incompreensível, que está cheio de oportunidades para os mais capazes, comporta riscos muito complexos que é necessário saber identificar, antecipar, controlar, antes que dêem origem a situações que podem ser irremediáveis.

Milhões de utilizadores, de todas as partes do mundo, estão inscritos em redes sociais virtuais. Por que o fazem? A questão deixa de ter lógica se pensarmos que a maioria dos utilizadores das redes virtuais é nativa digital (Prensky, 2001). São jovens que pertencem à primeira geração que nasceu e cresceu rodeada de diversos dispositivos tecnológicos (computadores, videojogos, música digital, câmaras de vídeo, telemóveis e toda uma panóplia de artefactos digitais). Esta nova geração pensa e opera num mundo largamente ocupado pela tecnologia e pelas redes sociais, para quem esta realidade não é um fenómeno mas sim o próprio dia a dia. Os jovens apropriaram-se das redes sociais das formas mais diversas, criando espaços de interacção muitas vezes incompreensíveis para os mais velhos, mas que são autênticos universos paralelos em que se movem à

vontade e protegidos dos olhares dos adultos, nomeadamente pais e professores. Os jovens são dos grupos mais vulneráveis do mundo digital, pela sua tendência natural para desvalorizar os riscos e para sobrevalorizar a sua capacidade de os identificar e lhes dar resposta.

São conhecidas muitas tentativas de criação de redes sociais que não tiveram muito sucesso, como *Friendster*, *MySpace*, *hi5*, entre outras, e sabe-se que a penetração de uma rede social varia de país para país, por razões que dependem de factores nomeadamente culturais (Winkels, 2013). As redes sociais preferidas dos jovens, entretanto, vão mudando com grande velocidade, deixando os adultos perdidos num espaço virtual que não dominam. Quando num esforço maior encontramos pais a registarem-se no *facebook* numa tentativa de compreenderem o fenómeno e acompanhar os filhos, assistimos à expansão de outras redes, completamente abertas, de que esses mesmos pais nunca ouviram falar e nem supõem que os filhos estejam registados, o que dizem, o que publicam, como se expõem... (Duggan, 2013).

Neste artigo, olhamos para os riscos e para a sua possível prevenção e visitamos uma rede social específica, considerada hoje em muitos países como uma rede onde os jovens enfrentam riscos e que pode, inclusivamente, ser letal quando usada como arma de assédio.

1. Os riscos

Numa leitura superficial, os utilizadores encaram as redes sociais como um espaço onde estão em contacto com os amigos, alguns distantes fisicamente por via das circunstâncias, contacto com grupos de interesse, entre outros, pelo que a evidência cronológica do que fazemos ou do que os amigos fazem é relevante para o indivíduo. Constroem efectivamente uma identidade, ao mesmo tempo que deixam no esquecimento a vulnerabilidade a que as pessoas (maiores ou menores de idade) se encontram expostas.

Estes espaços virtuais, em que a verificação da identidade é complexa, em que os jovens são na sua maioria ingénuos e predispostos a acreditar naquilo que lhes é dito, constituem terreno fácil para certos tipos de crime, que vão da chantagem ao assédio sexual, criando situações complexas que os próprios jovens, os pais e as escolas não estão preparados para enfrentar.

Hoje, o crime na *Internet* é altamente sofisticado e visa objectivos que vão desde o terrorismo internacional à lavagem de dinheiro, que precisam de se apoderar de largos milhares de computadores em rede para atingir os seus fins, às redes de tráfico de droga

e de crime sexual, ao assédio e/ou num universo mais local que se traduz muitas vezes em tragédias de que todos já ouvimos falar, a depressão, o baixo rendimento escolar, o suicídio.

Sem rigor na utilização, a *Web* transforma-se assim num “terreno fértil para predadores emocionais e sexuais, para burlões, para sofisticados piratas informáticos [e] grupos [...] que podem colocar em causa a segurança” (Almeida, 2009: 63). Urge, portanto, por um lado, a sua regulação – formal – e, por outro, formar alunos, professores e pais para que usem a *Web*, em particular as redes sociais, de forma prevenida, partilhando o que deve ser partilhado, e rentabilizando o lado bom da inteligência colectiva que aí vive.

2. A pegAdA dIgItAl

O conceito *Web 2.0* e o entendimento da *Web* como plataforma fez nascer a possibilidade de produzir conteúdos, publicá-los e partilhá-los sem que para isso sejam necessários conhecimentos técnicos especializados. Este acrescentar valor à *Web* que já O'Reilly (2005: 3) diz ser “one of the key lessons of the Web 2.0 era is [...] : Users add value” fica mais claro se pensarmos que a evolução das plataformas tem permitido que, desde muito cedo, cada indivíduo tenha uma *e-vida*. Muitas vezes, esta vida virtual não resulta da opção do próprio indivíduo, mas da vontade de alguém que, sobre ele, tem poder. Vejamos que são publicadas em *websites*, blogues, redes sociais, etc., fotografias de bebés, sem que estes, naturalmente, se pronunciassem sobre isso. Esta discussão precisa de ser feita, embora não seja o propósito específico deste trabalho. Antes, importa perceber que a vida virtual de milhares de utilizadores começou muito cedo, muitas vezes antes sequer de ocorrer por vontade própria. Neste ponto, devemos saber que toda a informação está na *cloud* (armazenamento de dados em computadores e servidores interligados por meio da Internet) e que um simples “apagar” ‘local’ não garante que essa informação simplesmente desapareça (desses servidores). É como que esta saísse da superfície, mas se mantivesse num nível mais “profundo”. A este propósito, Bergman (2001) tem um apontamento curioso comparando a pesquisa na *Internet* com uma rede piscatória. Ela apanha o que está à superfície, mas não garante que escape outra informação, num nível inferior, que a rede pode não alcançar, mas está lá, à mercê de alguém que, com conhecimentos, vontade e persistência, consiga encontrar (v. figura 1).

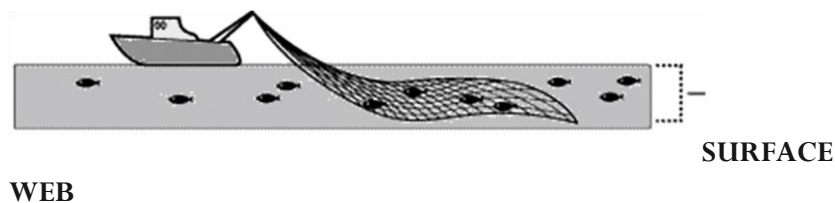


Figura 1. Motores de busca: Arrastar sobre a superfície da Web (Bergman, 2001)

Segundo Bergman (2001), “*most of the Web’s information is buried far down on dynamically generated sites, and standard search engines never find it...The deep Web is qualitatively different from the surface Web. Deep Web sources store their content in searchable databases that only produce results dynamically in response to a direct request. But a direct query is a “one at a time” laborious way to search*” (p. 1-3)”. As bases de dados estão lá, debaixo de um nível de interface com o utilizador, como é, por exemplo, a base de dados de informações fiscais. Tudo está lá, nessa *Web* profunda, escondida da maioria, mas acessível a alguns.

Também Acquisti (2013), da Carnegie Mellon University, estudou ‘economicamente’ a privacidade (e a segurança da informação) nas redes sociais. Para o economista, “*any personal information can become sensitive at some point!*” (2013, s.p.). Segundo Acquisti, no ano 2000 foram colocadas 100 biliões de fotos apesar de apenas uma ínfima parte ter sido colocada na *Web*. No entanto, em 2010, só num mês foram carregadas no Facebook 2,5 biliões de fotos, estando a maioria identificada (Acquisti, 2013). Ora, numa altura em que a tecnologia computacional facilmente possibilita identificar as pessoas nas fotografias ou mesmo através de informação disponível na *cloud*, esta competência que há alguns anos era apenas do domínio de agências governamentais, está agora ao dispor de qualquer utilizador da *Web*. Juntamente com a computação ubíqua, o resultado desta combinação de tecnologias implicará uma mudança radical nas nossas noções de privacidade e anonimato (idem, 2013). Pode-se partir de um rosto anónimo e usando tecnologia que permite o reconhecimento facial, dar um nome a esse rosto e saber informação pessoal publicada. É a *social media*.

A ideia de que tudo o que um utilizador faz, ou não faz, ao longo da sua vida nas redes sociais fica indelevelmente registado, começa a ser cada vez mais utilizada, por exemplo, por empresas de recursos humanos com um valor igual ao de um CV (*curriculum vitae*).

A pegada digital, o registo de tudo, rigorosamente tudo, que cada um faz e não faz na *Internet*, cada clique, estão hoje disponíveis praticamente a quem o queira, de uma forma legal. Veja-se, por exemplo, esta visualização realizada por *WolframAlpha.com*, do

dia da semana e hora do dia em que um determinado utilizador do *Facebook* costuma utilizá-lo.

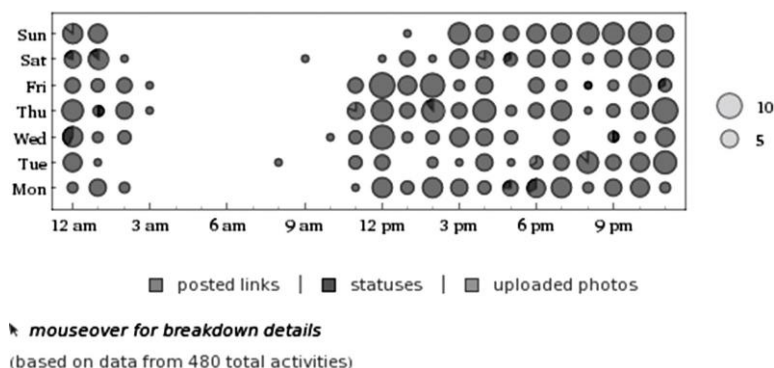


Figura 2. Registo da acção de um utilizador do *Facebook* (dia/hora) | *WolframAlpha.com*

A influência da pegada digital nas perspectivas de trabalho futuro, no recrutamento de recursos humanos, tem sido completamente esquecida. Quando um empregador precisa de recrutar alguém, antes mesmo de convocar um potencial funcionário para uma entrevista, a primeira opção passa por uma pesquisa simples no *Google* antes de proceder ao contacto pessoal. No estudo realizado por Acquisti (2013), numa amostra que dividiu em dois grupos, um dos quais publicou fotos de uma animada noite entre amigos e outro grupo que, não tendo publicado fotos suas, esteve em iguais condições, simulando uma situação de recrutamento de recursos humanos, o grupo que mais juízos de valor fez sobre aquelas, foi o grupo que não publicou fotos tendo-se mostrado mais relutante em chamar um candidato para uma entrevista, ainda que com “candidatos” com as qualificações pretendidas.

Um outro estudo em que participaram mais de 2000 consumidores e 600 empregadores revela que “one in five employers finds information about candidates on the Internet, and 59% of those said it influences recruitment decisions.[...] A fourth of human resources decision makers said they had rejected candidates based on personal information found online” (Ferguson, 2007: s.p). Apesar destes dados, a maioria das pessoas permanece ignorante sobre o efeito que a sua reputação na Internet pode ter nas suas perspectivas de emprego.

Deste modo, a pegada – e reputação inerente ao que é publicado – é construída de duas formas. Uma é ativa – os *blogs*, artigos, fotos, vídeos que cada indivíduo publicar. A outra é passiva - o que os outros colocam sobre cada um de nós. Kuhlen (2010) indica-nos que no *Twitter*, por exemplo, “the people following you can see who you are following and

check out what they are saying. Even though your tweets and retweets may be perfectly fine, your reputation can be affected by what others are saying or the language they are using — linked to you even though you are unaware and are not responsible for what is being said when your network is visible to others (p.68-69)”.

Mas estudos também reconhecem que muita da informação encontrada *online* também já funcionou positivamente na decisão de recrutar indivíduos (Ferguson, 2007: s.p).

Esta prática — *googling me/you* — é um exercício que cada um de nós pode fazer para perceber qual a marca que temos impressa. Uma pesquisa simples no Google em que cada indivíduo coloque o seu nome completo, com e sem aspas, oferece ao consumidor a imagem que pode ter de cada indivíduo. Essa imagem pode ter repercussões no campo pessoal e profissional: com mais ou menos impacto. A prevenção passa definitivamente pelo incremento da percepção de todos relativamente a todos estes riscos.

3. Facebook

O *Facebook* é hoje um ‘eco-sistema digital’ completo e complexo, com mais de 950 milhões de utilizadores, segundo *socialbakers.com*, dos quais 250 milhões na Europa, com uma taxa de penetração de 30%. O *Facebook* é um mundo virtual, plano, onde todos são iguais à partida e dispõem de idênticos recursos, pois uma vez registados podem, de uma forma intuitiva, escrever textos, partilhar objectos na sua linha do tempo, ver e comentar as linhas do tempo dos amigos. Tendo sido adoptada por centenas de milhões de utilizadores de todo o mundo como o espaço virtual, o *facebook* é a rede onde todos querem estar pela simples razão de ser aí que os seus amigos se encontram. Não obstante, importa conhecer alguns dados que apontam para a queda da primazia desta rede. De acordo com a pesquisa realizada pela empresa de consultoria *iStrategy*, entre Janeiro de 2011 e Janeiro de 2014, a rede perdeu mais de 6,7 milhões de jovens com idades entre 13 e 24 anos só nos Estados Unidos. A queda, salienta o jornal online G1 (2014), é ainda mais expressiva entre jovens com idades entre 13 e 17 anos, com a perda de 3,3 milhões.

Este manancial imenso de dados sustenta, por sua vez, o negócio do *Facebook*, que é na sua essência um negócio de publicidade personalizada. Importa estarmos conscientes que as informações pessoais sem grande ‘profundidade’ servem para que se possa traçar o perfil de um utilizador e com base nelas, empresas de *marketing*, por exemplo, estão habilitadas a apresentar o produto que, provavelmente, um utilizador considere útil, mesmo que não lhe seja necessário. Um exemplo que Acquisti (2013) nos apresenta é o

princípio que essas empresas, estudando o perfil de um utilizador e tendo acesso aos perfis dos amigos deste, através da criação de um algoritmo conseguem detetar dois dos melhores amigos desse utilizador. Essas empresas conseguem, em tempo real, criar uma composição facial desses dois amigos impedindo o reconhecimento imediato dessa “fusão facial”, mas conseguindo uma reacção positiva a essa composição. Empresas podem, assim, sugerir a compra de um produto por uma face aparentemente transformada mas cujos traços lhe inspiram confiança (afinal é a mescla das características físicas faciais dos seus melhores amigos!), induzindo-nos à compra sem que percebamos o modo como fomos ‘manipulados’.

Entretanto, uma maioria dos utilizadores não cuida devidamente da visibilidade do seu perfil pondo em causa a privacidade da sua vida pessoal e, por vezes, dos seus amigos.

Os jovens sabem utilizar melhor que os adultos estas definições de privacidade, sendo capazes de definir perfis que lhes permitem separar as atividades que os pais e professores podem ver daquelas que não!

Por diversas razões, os jovens aderem facilmente a comportamentos de risco, por curiosidade ou por necessidade de afirmação e, naturalmente, procuram outros espaços de comunicação e outras ferramentas onde estejam longe do alcance de quem os procura proteger, admitamos.

Estes espaços e estes comportamentos evoluem a grande velocidade, são fenómenos virais, imprevisíveis, que requerem uma atenção constante de quem os estuda. Há já quem defenda o afastamento total deste tipo de redes considerando como único meio de prevenção efetiva. Lembremos o que recentemente a Comissão Europeia recomendou aos cidadãos europeus: “*You might consider closing your Facebook account, if you have one*” por intermédio do advogado da Comissão, Bernhard Schima (Gibbs, 2015). Esta recomendação de fechar as contas no *Facebook* surge como forma eficaz de garantir que as informações pessoais ficam fora do domínio dos serviços de segurança dos Estados Unidos.

4. Ask.fm Recentemente, num inquérito realizado numa sala de aula de uma turma do 3º ciclo do ensino básico sobre plataformas *Web 2.0*, um número significativo de respostas indicou no campo ‘**outras**’ a plataforma *ask.fm* (Silva, 2013).

Esta resposta levou os autores a investigar um pouco esta plataforma e o que aí encontraram foi suficiente para os assustar e motivar para a escrita deste trabalho, tamanha é a pertinência desta realidade.

Também rapidamente verificaram que esta preocupação é mais generalizada e, por exemplo, no sítio *webwise.ie*, um sítio irlandês sobre segurança destinado a pais e professores, encontraram dois textos muito importantes: *Explained: What is Ask.fm?* e *Ask.fm Guide for Parents & Teachers*, que o mostram.



Figura 3. Guia para Pais e Professores sobre a *ask.fm* [Fonte: <http://ask.fm>]

Ask.fm é um sítio de perguntas e respostas, em que o utilizador pode colocar perguntas a outro utilizador ou ao universo de utilizadores, ou responder a essas perguntas. Há outros semelhantes, mas este aparentemente é o que conquistou os mais jovens em diferentes países.

As respostas podem ser partilhadas, os utilizadores podem construir o seu perfil e há ligações ao *Facebook*, *Twitter* e *Tumblr*, por exemplo.

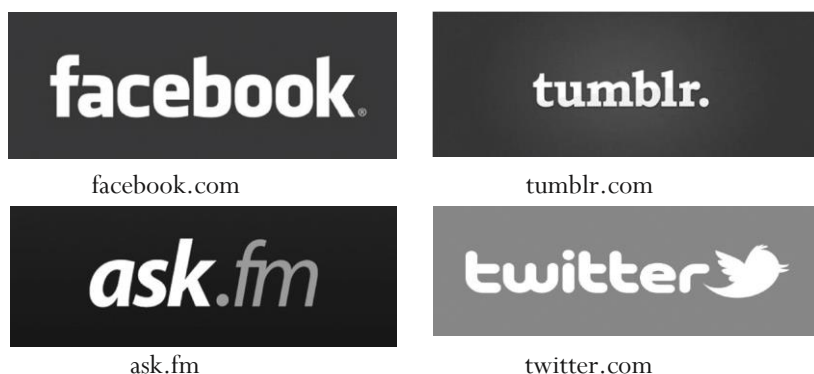


Figura 4. Redes sociais de grande utilização

[Fonte: facebook.com, tumblr.com, ask.fm.com e twitter.com]

O sítio é aberto, isto é, um utilizador não registado pode navegar pelas perguntas e respostas com poucas restrições e rapidamente se descobre que uma plataforma aparentemente inofensiva tem muitos conteúdos abusivos e sexistas, o que o torna um risco acrescido se tivermos em conta que o controlo da privacidade dos conteúdos é praticamente inexistente.

Os jovens, que por ingenuidade ou inconsciência se julgam afastados de criminosos (que vêm nestas redes oportunidades para levar a cabo os seus desígnios), são muitas vezes vítimas de armadilhas infernais para as quais só encontram uma saída. Veja-se o caso da jovem Hannah Smith, com 14 anos, que muito recentemente pôs fim à sua vida em consequência directa do assédio de que foi vítima através do portal *Ask.fm*. É apenas um entre os vários casos publicamente conhecidos e associados a essa rede.

Ainda recentemente, o jornal inglês *Mail Online* publicava que “*Pupils and parents warned over social networking website linked to teen abuse. - Schools across the country are sending out letters advising pupils not to use Ask.fm. - Site lets anyone see details of boys and girls as young as 13, then post comments or questions. - There is no way to report offensive comments. - Has become linked to a number of recent teen suicides.*”

Mas logo a seguir, o mesmo *Mail Online* dizia que “*Facebook ‘dead and buried’ as teenagers switch to WhatsApp and Snapchat - because they don’t want mum and dad to see their embarrassing pictures*”. E aqui todo um mundo de discussão se abre, da família, da educação, da escola, do respeito mútuo, que é absolutamente necessário discutir nos locais apropriados.

5. Construções de Identidade

“*But this is not a book about robots. Rather, it is about how we are changed as technology offers us substitutes for connecting with each other face-to-face*” (Turkle, 2012:1).

Uma pessoa hoje, digamos, ‘não existe’ se não tiver um perfil digital, no *Facebook* por exemplo, mas ao mesmo tempo não tem identidade própria se se afirmar apenas no *Facebook*. E aqui há um universo de subtilidades, de linguagens codificadas, de mundos impenetráveis, de culturas, que verdadeiramente só os próprios entendem. Partilhar fotografias no *Facebook*, no *Flickr*, no *Picasa*, no *Instagram*, no *Panoramio*, não são formas diferentes de fazer o mesmo, são coisas diferentes! Na verdade, são verdades dinâmicas e universais, que não se ensinam, aprendem-se. Colocar vídeos no *YouTube* ou no *Vimeo* visam objectivos diferentes. Ter um blogue, ter uma conta no *WordPress*, ter uma página

no *Pinterest*, não são alternativas. As escolhas, as opções, fazem parte da identidade individual, tal como a cor da roupa ou o corte do cabelo.

A plataforma *Google+*, que procura, através de uma diferenciação nítida, conquistar um segmento de público mais esclarecido, que pretende outras formas de socializar, sem as interferências de jogos sociais, de excessos de comentários, de repetições de partilhas, que hoje caracteriza aquela rede social, posicionou-se como o grande rival do *Facebook*. O *Google+* constrói-se à volta da ideia de círculos, de amigos, de conhecidos, de pessoas interessantes, etc. e da integração de plataformas do universo Google, nomeadamente, o serviço *Gmail*.

No entanto, esta aposta está a falhar, nomeadamente entre os jovens. Num estudo recente, verificou-se que redes mais efémeras como o *Instagram* ou o *Snapchat* estão a ganhar a batalha.

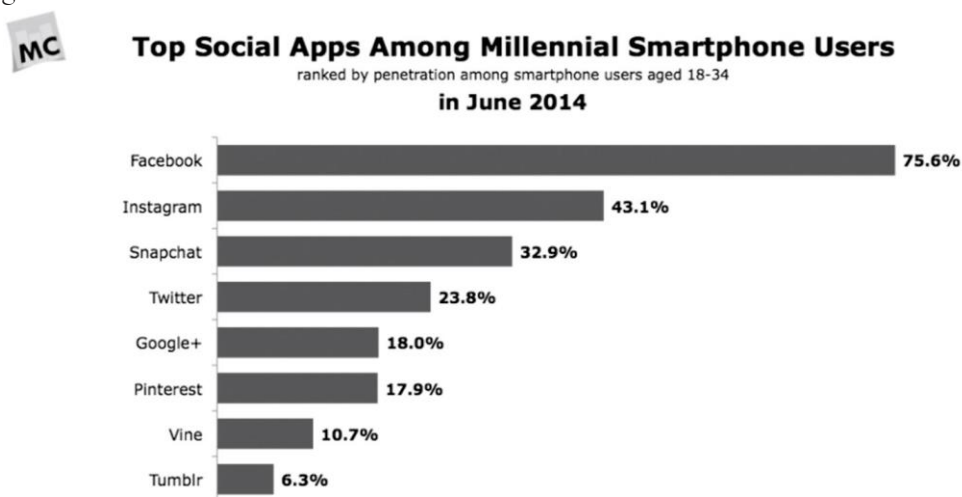


Figura 5. Top das *Social Apps* mais usadas pelos utilizadores de smartphones
[Fonte: MarketingCharts.com, comScore]

Observações recentes mostram que em Portugal a evolução não será muito diferente, apesar de duas redes sociais universalmente muito utilizadas, o *Twitter* e o *LinkedIn*, ver a sua aceitação esbarrar com o espírito bem português de não gostar da ideia de dar para receber...

6. A prevenção

“Before the permanence of the digital record of our lives, most of what we did as children was forgotten beyond anecdotes of parents and friends — and forgiven. That is a luxury not available to today’s children. Our professional responsibility is not only to own our professional online identity and reputation, but to understand enough that we can provide advice and be an online model for our students” (Kuhlen, 2010: 69).

No terreno da prevenção, o papel de pais e professores torna-se ainda mais crucial do que, arriscamos dizer, alguma vez foi. Nas sociedades de outros tempos, não muito distantes aliás, pais e professores procuravam junto dos jovens formá-los para serem bem sucedidos na sociedade, como se esta resultasse de um estado pouco mutável. Mas a explosão dos *mass media* e consequente possibilidade de produzir e publicar para a *Web* destronou essa realidade: não basta ser formado para ser bem sucedido na sociedade. É preciso mais. É preciso ser — o mais precocemente possível — consciente da realidade em que nos movemos e agir nela de forma responsável, segura e com uma intervenção positiva.

Cabe aos pais e professores consciencializarem os jovens sobre o potencial da *Web 2.0* e das redes sociais, mas sobretudo ajudar os jovens a conhecer e a gerir a sua pegada digital. Estes agentes, num trabalho que deve ser pensado em conjunto, devem ser capazes de fazer entender aos jovens que o modo e o mundo onde se movem nas redes sociais têm impactos efectivos. O problema é que os jovens, os criadores de plataformas *Web*, os que estudam afincadamente os comportamentos dos jovens, estão bem à frente dos pais e professores na compreensão e na apropriação de novas ferramentas. Talvez se possam aqui inverter os papéis e levar os jovens, os alunos, a ensinar os pais e os professores dos modos de utilizar e dos perigos destas plataformas.

Plataformas como o *Tumblr*. ou o *Twitter* têm características próprias em matéria de comportamentos que escapam ao observador menos atento, que as considerará no grupo geral de redes sociais, enganando-se seriamente na compreensão do que leva os jovens mais embebidos nas redes a adoptá-las em detrimento do *facebook*, por exemplo.

Um estudo feito com todos os alunos do 9.º ano de uma escola do norte do país, num total de 124 participantes, conclui que a maioria utiliza várias redes sociais, frequentam-nas diariamente, principalmente por lazer, diversão e partilha de ficheiros, mas indica-nos que, apesar de terem consciência da informação que deve ou não ser publicada, ignoram esse conhecimento uma vez que continuam a partilhar informação potencialmente perigosa, não tendo percepção clara que a informação publicada é

permanente e pode vir a ter impacto no futuro, nomeadamente a nível profissional (Silva, 2013).

A escola deve, na sua missão de dar a conhecer, modelar os jovens também no que respeita à marca que deixam na *Web*, nomeadamente, esclarecer a ignorância que parece latente sobre o modo como a actuação na *Web* e em particular nas redes sociais podem ter um impacto negativo no futuro, particularmente na reputação profissional. Devem estes agentes trabalhar no sentido de consciencializar os jovens da importância de criarem e gerirem a sua pegada digital, de modo a que esta marca esteja protegida e constitua uma mais-valia para a sua reputação pessoal e profissional. Consciencializar os jovens que a partilha de informação pessoal com o mundo tem um impacto que pode ir para além do imediato é urgente.

Como nos indica Dolan (2009): “*students today have been using social networking sites since they were teens...It’s been talked about, but there really hasn’t been a concerted effort by churches, schools, social organizations to really teach people how to use these tools appropriately and inappropriately*” (2009: 8). Corroboramos com a autora nesta ideia de que as diversas entidades devem agir localmente num pensamento global. Como os nossos jovens estão mais tempo na escola do que em casa, a missão de consciencializar os jovens desta realidade e dos riscos a ela associados cabe, em primeira mão, aos seus professores.

A tarefa está longe de ser fácil, porque a prevenção destes crimes é muito difícil, pois coloca dum lado adultos que não compreendem muito bem os processos que estão por trás destes fenómenos e, do outro, os jovens, que têm tendência para pensar que tudo não passa de exageros dos adultos.

Assim, só há uma forma de os jovens entenderem estes problemas, e que consiste em levá-los à descoberta da realidade do risco nas redes sociais, das portas que todos deixam abertas todos os dias na sua utilização normal dessas redes, da forma como essas portas são utilizadas por criminosos para atingir os seus objectivos.

Desde um clique que um faz numa mensagem de correio electrónico aparentemente pacífica, uma fotografia que se disponibiliza sem se pensar previamente nas suas consequências, à resposta a uma simples pergunta feita por um desconhecido, tudo são portas que pessoas mal-intencionadas podem utilizar para concretizar os seus intentos.

Estes problemas não têm solução simples, mas tudo passa pela actuação concertada dos três pilares da educação dos jovens – a família, a escola e a sociedade. E o primeiro passo será certamente colocar estes problemas na ordem do dia e criar um espaço de diálogo em que pais e filhos aprendem em conjunto a melhor forma de enfrentar estes problemas no dia a dia. É este um dos grandes desafios da educação hoje.

Conclusão

A *Web*, em particular as redes sociais, passou a ser um instrumento de comunicação por excelência entre pessoas sem que estas se vejam ou, sequer, se conheçam e sem que se interroguem sequer sobre quem suporta os custos da sua disponibilidade. Escapa às pessoas que a matéria-prima essencial das empresas que operam neste mercado são exactamente os dados pessoais e de consumo dos milhares de milhões de utilizadores do *Google*, do *Facebook*, *Ask.fm* e das outras plataformas, que foram construídas para captar esses dados pessoais, não obstante permitirem ao utilizador consciente e experimentado um controlo razoável daquilo que disponibiliza ao seu círculo de amigos e ao público em geral.

As redes sociais revelam-se um terreno fácil para que utilizadores mal intencionados posam aproximar-se de pessoas menos preparadas para enfrentar este tipo de ameaças e cometerem os mais variados tipos de crimes. Cabe aos agentes sociais com obrigações declaradas (pais, escola, autarquias, paróquias, etc...) uma intervenção activa e eficaz, cabe a eles deixarem de ter comportamentos parecidos às avestruzes – ignorando o que se diz, escreve ou publica *online* - e passar a ter olhos de águia para inspecionar os ambientes digitais e responder às necessidades e ameaças (Hengstle, 2012). Segundo a autora, “*regardless of whether educators decide to actively manage their own digital footprint, they have a moral responsibility to teach students how to manage their digital footprints to protect and hopefully expand the students’ future opportunities* (2012: 92). Esta responsabilidade moral não deve ser relegada para segundo plano. É crucial que os professores desde os primeiros anos do ensino básico trabalhem com os seus alunos a sua pegada digital e que os tornem conscientes e conscienciosos do que publicam, quer publiquem sobre si, quer publiquem sobre outros. Mas, para isso, precisamos de professores esclarecidos e formados sobre os riscos e a criminalidade que podem ocorrer nestes meios. **referências bibliográficas**

Almeida, P. (2009). Redes virtuais são espaço sem lei. In *Diário de Notícias*. Disponível em

http://www.dn.pt/inicio/opiniao/interior.aspx?content_id=1219447&secao=Pau [consultado em 11/01/2013].

Acquisti, A. (2013). Why privacy matters. TED Speakers. Disponível em

http://www.ted.com/talks/alessandro_acquisti_why_privacy_matters.html [consultado em 11/11/2013].

Bergman, M. (2001). White paper: The deep web: Surfacing hidden value. *The Journal of Electronic Publishing*, 7(1). Disponível em <http://dx.doi>.

org/10.3998/3336451.0007.104 [consultado em 1/03/2013].

Dolan, P. (2009). Social media behavior could threaten your reputation, job prospects. *American Medical News*. Disponível em <http://www.ama-assn.org/amednews/2009/10/12/bil21012.htm> [consultado em 1/03/2013].

Douglas, N. (2007). *How to look good when your recruiter Googles you*. Disponível em <http://valleywag.gawker.com/tech/silicon-valley-users-guide/how-to-look-goodwhen-your-recruiter-googles-you-247854.php> [consultado em 5/03/2013].

Duggan M., Smith A. (2013) Social Media Update 2013. Disponível em <http://www.pewinternet.org/Reports/2013/Social-Media-Update.aspx> [consultado em 3/1/2014].

Ferguson, T. (2007). *Want a job? Clean up your Web act*. Disponível em http://news.cnet.com/2100-1025_3-6171187.html [consultado em 5/03/2013].

Gibbs, S. (2015). Leave Facebook if you don't want to be spied on, warns EU. In *The Guardian*. Disponível em

<http://www.theguardian.com/technology/2015/mar/26/leave-facebook-snooped-on-warns-eu-safe-harbour-privacy-us> [consultado em 01/04/2015]. Hengstler, J.

(2012). Managing digital footprints: Ostriches v. eagles. In S. Hirtz & K. Kelly (Eds.), *Education for a digital world 2.0* (2nd ed.) (Vol. 1, Part One: Emerging technologies and practices). Open School/Crown Publications: Queen's Printer for British Columbia, Canada. Disponível em

http://order.openschool.bc.ca/Product/CourseDetail/search_education%20for%20a%20digital%20world_7540006163 [consultado em 4/03/2013].

Kaplan, A. M. & Haenlein, M. (2010) Users of the world, unite! The challenges and opportunities of Social Media, *Business Horizons* (2010) 53, 59 - 68.

Kuehn, L. (2010). *Manage your digital footprint*. *Teacher Newsmagazine*, 23(3). Disponível em http://www.policyalternatives.ca/sites/default/files/uploads/publications/National%20Office/2012/02/osos106_Digital_Footprint.pdf [consultado em 4/03/2013].

Office/2012/02/osos106_Digital_Footprint.pdf [consultado em 4/03/2013].

O'Reilly, T. (2005). *What is Web 2.0*. O'Reilly. Disponível em <http://oreilly.com/web2/archive/what-is-web-20.html> [consultado em 1/03/2013].

- Prensky, M. (2001). *Digital Natives, Digital immigrants*. Disponível em <http://www.marcprensky.com> [consultado em 14/02/2013].
- Silva, P. (2013). Pegada e Identidade Digital – um estudo de caso no âmbito da Prática de Ensino Supervisionada. Dissertação do Mestrado em Ensino de Informática - Faculdade de Ciências Sociais - Universidade Católica Portuguesa.
- Turkle, S. (2012). *Alone Together: Why We Expect More from Technology and Less from Each Other*, Basic Books.
- Winkels, M. (2013). The Global Social Network Landscape: A Country-by-Country Guide to Social Network Usage, eMarketer, Julho 2013.
- Webwise (2013), *Explained: What is Ask.fm?* Disponível em <http://www.webwise.ie/AskFMExplained.shtm> [consultado em 3/03/2013].
- Ask.fm Guide for Parents & Teachers*. National Centre for Technology in Education. Disponível em <http://www.ncte.ie/News/Mainbody,22520,en.html> [consultado em 3/03/2013].
- G1 – Tecnologia e Games (2014). Milhões de jovens abandonam o Facebook. <http://g1.globo.com/tecnologia/noticia/2014/01/67-milhoes-de-jovens-abandonamfacebook-em-3-anos-diz-pesquisa.html> [consultado em 1/04/2013].