



TEÓRICAS 3

As Redes Sociais na Internet

▣ O que são as redes sociais?

Depois das férias, aqui estamos com um novo resumo para os pais. Desta vez referente à terceira *Ficha de Apoio* disponibilizada aos professores.

O tema “AS REDES SOCIAIS” é, sem dúvida, um dos mais preocupantes já que elas são, em todo o mundo, o local eleito pelos mais novos para as suas peregrinações **online**, permitindo-lhes criar, com a maior facilidade, páginas pessoais onde disponibilizam o seu perfil (a maior parte das vezes, recheado de excessivas informações, fotografias e vídeos) e proporcionando a comunicação entre os vários membros da Rede através de *blogs* ou mensagens instantâneas.

Mas afinal o que são as redes sociais?

As redes sociais na Internet – conhecidas por *Social Networking Sites (SNSs)* ou *Online Social Networks* partilham interesses e actividades, de modo geralmente gratuito e imediato, estabelecendo relações assentes na afinidade de gostos, ideias ou acções.

Os *sites* que disponibilizam estas redes sociais estão, actualmente, entre os mais visitados do mundo, tendo-se transformado num dos fenómenos tecnológicos mais notáveis do século XXI.

Entre as mais conhecidas redes sociais encontram-se o Hi5 (muito utilizado em Portugal), MySpace, Facebook, Flickr, Friendster, Orkut, MSN Spaces e You Tube.

Quantidades gigantescas de informação pessoal, especialmente fotografias e vídeos, tornaram-se pública e globalmente disponíveis de uma forma sem precedentes.

Um dos maiores desafios que se colocam à privacidade é o facto de a maioria dos dados pessoais publicados numa rede social o serem por iniciativa do próprio utilizador, contando assim com o seu consentimento.

Embora as redes sociais ofereçam uma nova gama de oportunidades de comunicação e troca de informações, podendo ser de grande utilidade até a nível educativo, a sua utilização comporta sérios riscos para a privacidade dos seus utilizadores.

□ Informação pessoal que nunca desaparece

É extremamente importante que os jovens se apercebam que a noção de “esquecimento” não existe na Internet. Uma vez publicados, os dados permanecem lá para sempre. Mesmo que apagados, os serviços de arquivo na Internet conservam toda a informação. Com pouco esforço, esses dados podem sempre ser acedidos.

É, por isso, imprescindível terem bem presente que, a partir do momento em que se publica o nome, o telefone, a morada, as fotos da festa, as actividades, os desejos, os medos, o diário do que se fez, a religião, a orientação sexual, etc., se está a disponibilizar informação que muito dificilmente alguma vez deixará de estar acessível.

Passados 10, 20 ou 40 anos, ao fazer uma pesquisa sobre um nome (por exemplo), aparecerá toda a informação que lhe está associada, podendo vir a ter um efeito absolutamente perverso na realidade pessoal e profissional das pessoas, penalizando-as por actos ou opções praticados numa fase da juventude, em que a ingenuidade e o normal desejo de transgressão conduzem, frequentemente, a uma excessiva exposição.

□ A falsa noção de “comunidade” e de “amigos”

Atenção, também, à ilusão de intimidade que as redes sociais criam, promovendo a partilha de informação *online*, num clima de grande confiança.

Ora esta ideia é claramente falaciosa, na medida em que nestas “comunidades” muitos dos “amigos” são uma incógnita. Facilmente se coleccionam centenas de amigos digitais, aumentando os índices pessoais de popularidade, que podem funcionar para os jovens como um bálsamo de auto-estima e satisfação.

Mas, na verdade, podem estar a partilhar informações sobre si, os seus amigos reais ou a sua vida familiar com um número incalculável de desconhecidos, não controlando quem efectivamente acede a todo esse manancial de dados pessoais e o que pode vir a fazer com eles.

□ Disponibilização excessiva de dados pessoais (fotos)

Criar um perfil numa rede social é muito simples, não exigindo grande destreza técnica. A idade mínima normalmente exigida pelos serviços de redes sociais é de 13 anos. No entanto, como não existe qualquer controlo efectivo sobre a idade dos subscritores, qualquer criança pode abrir a sua conta.

Basta ter um endereço de correio electrónico para a criar. A partir daí, é só preencher um formulário para criar um perfil. Em muitos casos, os miúdos disponibilizam, logo à partida, o seu nome verdadeiro, a sua localização (morada, telefone, escola, turma, etc.) bem como um conjunto de outra informação de natureza pessoal sobre as suas opções, o seu percurso, a sua vida familiar, os seus gostos, etc.

De igual modo, a possibilidade que as redes sociais oferecem de ligar as fotografias a nomes, perfis ou endereços de correio electrónico, coloca riscos adicionais para a privacidade.

▣ Cruzamento de informações

Os prestadores de serviços de redes sociais são tecnicamente capazes de registar cada acção, cada movimento que é feito no seu *site*. Deste modo, é possível também detectar as redes de contacto de cada utilizador, sabendo quem se relaciona com quem. Estes dados, associados à informação pessoal publicada em cada perfil individual, são extremamente apetecíveis para efeitos de marketing, em especial marketing dirigido a determinados públicos-alvo.

A necessidade crescente de financiar estes serviços e de apresentar lucros leva à recolha e utilização dos dados pessoais dos utilizadores para outros fins, designadamente a sua venda a empresas comerciais.

▣ Spam e vírus

As redes sociais tornaram-se ambientes de eleição para a propagação de *spam* (mensagens electrónicas não solicitadas para fins de marketing), quer através de convites automáticos para “amigos”, quer através da publicação de comentários automáticos, que remetem para *sites* de publicidade ou de pornografia. Os

spammers criam falsos perfis integrando-se nas redes e usufruindo destas ferramentas para chegar ao maior número possível de pessoas.

As redes sociais, devido à sua estrutura interligada, constituem locais privilegiados para ataques de vírus, que se propagam com uma rapidez espantosa, infectando milhões de perfis. Esta vulnerabilidade pode ter como consequências adicionais a exposição do perfil individual, a diversão para um ataque de *phishing*¹, o envio de conteúdos não solicitados por correio electrónico e por mensagens instantâneas.

☐ Ameaças sociais

As redes sociais são especialmente vulneráveis a situações de perseguição (*stalking*²) e de ameaça, dano ou ofensa (*cyberbullying*³).

Dados estatísticos disponíveis indicam um crescimento do fenómeno do *cyberbullying*, a partir das redes sociais.

O impacto do *cyberstalking* na vítima pode variar entre a intimidação moderada e perda de privacidade e a ofensa física grave e danos psicológicos.

O comportamento de *cyberbullying* pode revestir-se de muitas formas mas tem, quase sempre, consequências devastadoras para as suas vítimas.

¹ **Phishing** – esquema fraudulento, realizado através de mensagens electrónicas, cujo remetente se apresenta com uma falsa identidade (de uma pessoa, empresa ou instituição existentes), com o objectivo de levar o destinatário a fornecer dados pessoais que serão usados posteriormente para roubo de identidade.

² **Stalking** – perseguição que envolve um comportamento ameaçador, no qual o perpetrador procura repetidamente contacto com uma vítima através de proximidade física e/ou chamadas telefónicas, mas também através de meios electrónicos, como o correio electrónico (e-mail), mensagens instantâneas e mensagens nas redes sociais (*cyberstalking*).

³ **Cyberbullying** – termo usado para descrever actos intencionais e repetidos de ameaça e ofensa, através da utilização de tecnologia, em particular dos telemóveis e da Internet.

▣ Utilização indevida dos dados do perfil pessoal por terceiros

Um dos maiores riscos das redes sociais relaciona-se com as ameaças à identidade da pessoa. A grande quantidade de dados pessoais disponível nos perfis de utilizador potencia o roubo de identidade através da apropriação de perfis por terceiros mal intencionados.

As redes sociais facilitam, pelas debilidades de segurança da sua própria infraestrutura, os ataques de *phishing* personalizados.

A recolha fácil de dados nos perfis pessoais e nos respectivos círculos de “amigos” – que visam a obtenção de *usernames* (nomes de utilizador) e *passwords* (palavras-passe) - permite personificar o utilizador e agir em nome dele, o que significa roubar a sua identidade, podendo levar a cabo um conjunto de acções de consequências imprevisíveis: prejuízo da sua reputação, dano financeiro, envolvimento em actividades criminosas.

Setembro 2008