Para citar este artículo:

Caetano, H., Miranda, G. L. e Soromenho, G. (2010). Comportamentos de risco na internet: um estudo realizado numa escola do ensino secundário, *Revista Latinoamericana de Tecnología Educativa - RELATEC*, 9 (2), 167-185. [http://campusvirtual.unex.es/revistas/index.php?journal=relatec]

Comportamentos de risco na internet: um estudo realizado numa escola do ensino secundário

Internet risk behaviours: a study developed in a secondary school

Henrieu Caetano, Guilhermina Lobato Miranda e Gilda Soromenho

Instituto de Educação
Alameda da Universidade
1649-013- Lisboa - Portugal

Universidade do Lisboa

Email: e-caetano@sapo.pt; gmiranda@ie.ul.pt; gspereira@ie.ul.pt

Resumo: A questão da segurança na utilização da Internet tem sido alvo da atenção dos meios de comunicação social que realçam, fundamentalmente, os perigos do seu uso por parte dos jovens. Também nos deparamos nas escolas com alguns casos problemáticos relacionados com a utilização incorrecta dos computadores e da Internet, nas vertentes técnica e ética e ainda em certos comportamentos de risco que poderão ter consequências nefastas. Julgamos importante aprofundar este problema e estudar a sua dimensão numa escola do ensino secundário situada na região de Lisboa para, com base neste conhecimento, delinear um projecto de intervenção. Após uma revisão cuidada da literatura, optámos por uma investigação por questionário, fazendo a adaptação de três versões: uma destinada aos jovens, outra aos pais e outra aos docentes. Os resultados a que chegámos, nesta primeira fase do estudo, apontam para que alguns alunos têm comportamentos de risco, havendo a registar comportamentos agressivos, publicação de informações pessoais e a exposição de uma forma que pode trazer incómodos futuros. Verificou-se ainda que, quase sempre, os comportamentos potencialmente perigosos são praticados em casa, havendo respostas contraditórias por parte de encarregados de educação e alunos no que respeita aos limites de tempo para aceder à Internet e ao grau de supervisão durante o acesso.

Palavras-chave: Internet; Comportamento; Risco; Segurança; Comportamentos de risco online; Comportamentos seguros online

Abstract: Safe Internet use has attracted the focus of media attention, particularly due to its dangers for young people. As teachers, we have encountered some problematic cases in our daily lives related both to technical and ethical Internet misuse as well as other risky behaviours that may have adverse consequences. The

aim of this study is to understand such misuse and intervene accordingly in a secondary school near Lisbon. After a detailed review of the literature, we opted for a questionnaire type of research, based on the adaptation of three versions: one for young people, another for parents and another for teachers. The results we found in this initial phase of the study indicate that some students have risky behaviours, such as aggressive behaviour, the publication and exposure of personal information in a way that can cause some discomfort in the future. It was also found that potentially dangerous behaviors are almost always practiced at home, with contradictory responses on the part of parents and students with regard to time limits for Internet access and the degree of supervision during such access.

Keywords: Internet; Behaviour; Risk; Safety; Risky online behaviours; Safe online behaviours

1. Introdução

A decisão de realizar uma investigação sobre este assunto foi devida, entre outros factores, ao facto de as tecnologias da informação e comunicação serem um instrumento de utilização corrente por parte dos alunos e ser para nós desconhecida a atenção que estes dispensam às questões de segurança na sua utilização. Os resultados serviram ainda para delinear um projecto de intervenção, envolvendo os órgãos de gestão da escola, professores, pais e alunos. Pensamos que o desenvolvimento de projectos e programas deve basear-se num conhecimento o mais objectivo possível da realidade e não em pressuposições e preconceitos. Estes devem ainda ser avaliados recorrendo a medidas objectivas de impacto e de processo. Neste artigo vamos reportar os resultados da primeira fase do projecto, que designamos de caracterização da realidade ou baseline.

A Internet não é, na sua essência, controlada por qualquer entidade concreta (Silva e Remoaldo, 1997). O facto de não haver um controlo centralizado faz parte do fascínio da Internet: podemos, de uma forma geral, dizer e escrever o que quisermos para uma audiência de milhões e termos acesso às opiniões dos outros, pessoas comuns como nós. No entanto, esta falta de controlo pode trazer alguns dissabores, tais como sermos confrontados com conteúdos que consideramos abusivos ou ofensivos, quando não o esperávamos.

No que respeita à utilização da Internet e no aproveitamento que esta rede nos oferece, muitas vezes são as crianças que têm vindo a rasgar novos horizontes, com os adultos a segui-las ansiosamente (Turkle, 1995). Aliás, muitos adultos concordam que o seu comportamento relativamente aos computadores revela sintomas que um psicólogo escolar poderia classificar como dificuldades de aprendizagem (Papert, 1996:29).

2. Os riscos online

Segundo Ponte & Vieira (2008), é maior o risco da não utilização da Internet do que o risco da sua utilização. No entanto, se as vantagens são muitas, também os perigos são sérios (Papert, 1996). Alguns riscos associados à Internet são (Comissão Europeia, 2008):

- Cyber-bullying: Ao contrário do bullying, o cyber-bullying envolve a utilização das tecnologias e pode durar todo o dia, portanto o adolescente em causa pode estar exposto na escola e em casa, durante os períodos lectivos e durante as férias. Pode incluir comportamentos como enviar mensagens de texto, colocar fotografias embaraçosas online, espalhar boatos na Internet e outros. Tanto no bullying como no cyber-bullying as vítimas e os provocadores podem ser indivíduos ou grupos.
- Perda da privacidade;
- Eventual perda de segurança física associada ao facto de terem sido divulgados dados como horários escolares, moradas, fotografias, entre outros;
- Recepção de material pornográfico, xenófobo ou de violência extrema, enviado por desconhecidos ou até por amigos próximos;
- Visualizar conteúdos embaraçosos sobre os seus amigos ou sobre si próprio nos perfis dos seus amigos nas redes sociais;
- Ser vítima de fraudes online;
- Ser "bombardeado" com mensagens de ofertas e outras publicidades não solicitadas;
- Aliciamento para o jogo a dinheiro online.

Existem outros perigos, que podem afectar todos os utilizadores, como por exemplo:

- Vírus: programas que contém instruções que o computador irá executar e que têm a capacidade de se auto-replicar e infectar outros computadores (Oliveira, 2000);
- Troianos: programas que têm uma finalidade escondida, diferente daquela que anunciam. Muitas vezes permitem o controlo do computador através da Internet sem que o utilizador se aperceba. São exemplos o Netbus e o BackOrifice (Oliveira, 2000);
- Phishing e Pharming: tentativa ilícita de apropriação de dados pessoais (BES, 2009), sendo estes fornecidos pelo utilizador, quando julga que está a aceder a um local que é genuíno e na realidade está a aceder a um local que é uma imitação;
- Spyware: software que recolhe informações pessoais sem primeiro informar que o está a fazer, e sem que se possa decidir se se aceita ou

> recusa. As informações que o spyware recolhe podem ir desde informações relativas a todos os sites que se visitou, até informações mais sensíveis, tais como nomes de utilizador e palavras-passe (Santander-Totta, 2008).

Segundo Ponte (2008), Portugal é um dos países onde as crianças e jovens utilizam mais as tecnologias do que os adultos e os pais portugueses são dos que menos conhecem os hábitos dos seus filhos enquanto navegam na Internet. Esta autora refere ainda que os pais portugueses julgam que as crianças mais novas correm mais riscos do que as mais velhas e que as raparigas correm mais riscos que os rapazes. No entanto, as pesquisas indicam que as crianças mais velhas exploram mais a Internet e portanto estão mais expostas aos perigos e às oportunidades e, por outro lado, ambos os sexos tiram partido das potencialidades e estão sujeitas aos perigos num grau semelhante (idem). A Escola pode ter um papel central nesta questão, e tem como vantagem ser um local por onde passam todas as crianças e jovens.

Comunicar online comporta riscos, mas não devemos dramatizar ou exagerar esta questão. Na nossa vida fora da Internet também podemos ser importunados e também podemos conhecer pessoas desagradáveis. O que se pode fazer é tentar minimizar a probabilidade dessas situações acontecerem. Um ponto fundamental que deve ser focado quando se aborda a questão da segurança na Internet tem a ver com a questão técnica (Microsoft, 2010). A solução aconselhada para este problema passa por:

1. Manter o Sistema Operativo actualizado;
2. Utilizar uma firewall;
3. Usar um anti-vírus;
4. Fazer cópias de segurança com regularidade;
5. Evitar downloads de sites potencialmente perigosos (por exemplo de partilha de senhas de software);
6. Utilizar um programa anti-spyware também é recomendado, especialmente por instituições bancárias. As instituições bancárias recomendam que os acessos às contas sejam feitos apenas em computadores pessoais e não em computadores partilhados, de forma a minimizar a possibilidade de apropriação ilícita dos dados. Isto é válido para acessos a informação bancária ou outra (Santander-Totta, 2008).

De acordo com o sítio SeguraNet, que é dedicado ao uso esclarecido da Internet, e que é desenvolvido pelo Ministério da Educação, as três regras básicas para navegar de forma segura, são: Não revelar o «…nome, número de telefone, endereço, palavras-passe, ou quaisquer outras informações pessoais, mesmo que estas te sejam pedidas nos sítios Web que visitas». «Se algo que estás a ler ou a ver no computador te fizer sentir pouco à vontade, desliga-o». «Nunca aceites encontrares-te pessoalmente com alguém que conheceste online».

Segundo Wolak, Mitchell, & Finkelhor (2006) no YISS-2 (Youth Internet Safety Survey – 2, estudo realizado nos Estados Unidos), alguns comportamentos de risco são:

- Colocar informação pessoal em sítios públicos;
- Enviar informação pessoal a alguém que não se conhece pessoalmente;
- Falar sobre sexo com alguém que não se conhece pessoalmente;
- Aceder, propositadamente, a sítios pornográficos;
- Transferir para o computador, propositadamente, material pornográfico, através de sites ou mecanismos de partilha de ficheiros (como por exemplo o BitTorent);
- Utilizar um "nickname", ou alcunha com conotação sexual;
- Colocar ou enviar uma fotografia do próprio com cariz sexual;
- Fazer comentários ofensivos online;
- Utilizar a Internet para incomodar ou provocar alguém;
- Transferir ficheiros através de programas de partilha (como por exemplo, o BitTorrent);
- Colocar pessoas desconhecidas nos endereços de amigos, em programas de conversação (como por exemplo, MSN).

Wolak, Mitchell & Finkelhor (2006) consideraram informação pessoal, no YISS-2 (Youth Internet Safety Survey - 2), o seguinte: Nome verdadeiro, número de telefone, endereço postal, nome da escola que frequenta, idade, data de nascimento e fotografia.

É claro que enviar algo como a idade e a cidade onde se mora não terá qualquer risco, estando o risco associado ao conjunto das informações que possam, por exemplo, permitir a identificação do utilizador. A colocação online de fotografias, vídeos ou outras informações acerca do próprio pode trazer problemas a longo prazo, uma vez que depois de colocadas na Internet se perde o controlo sobre elas, podendo aparecer noutros sites mesmo depois de o autor as ter retirado.

O risco advém de um padrão de comportamentos. O facto de se ter uma página numa rede social, como o *Hi5* ou o *FaceBook*, não é, por si só, um factor de aumento de risco, pois este advém sobretudo de interacções com pessoas que são desconhecidas e cujos conteúdos são de cariz sexual (Wolak, Finkelhor, Mitchell & Ybarra, 2008). Ainda segundo estes investigadores, os jovens mais sujeitos a ter problemas online são aqueles que foram vítimas de maus tratos ou de abuso sexual, sendo que as raparigas são mais vulneráveis assim como os rapazes que são homossexuais ou que estão a questionar a sua identidade sexual.

Segundo McQuade III & Sampat (2008), os alunos estão mais sujeitos a serem vítimas de comportamento ofensivo online por parte de outros

estudantes do que por parte de adultos. Segundo Wolak et al. (2008), os adultos que se tentam aproximar de jovens na Internet para fins sexuais são em pequeno número quando comparado com o que existe no mundo físico, raramente incluem pedófilos e também raramente existem episódios de violência.

Em relação à problemática da protecção dos direitos sobre quaisquer obras em geral, literárias, científicas ou outras, colocam-se os mesmos problemas que se colocaram ainda antes da era da Internet: o plágio, a cópia não autorizada e a falsificação de obras. Apesar da legislação existente para a protecção dos direitos de autor, estes problemas sempre existiram e continuarão a existir com a diferença de praticar um acto ilícito ser mais fácil, rápido e com uma maior abrangência espacial (Ribeiro e Rosa, 2009).

A pirataria de programas de computador é um crime previsto na Lei da Criminalidade Informática (Lei 109/91 de 17 de Agosto), podendo ser aplicada uma pena de até três anos de prisão. Esta lei também prevê penas para acesso ou tentativa de acesso ilícito a sistemas informáticos, intercepção de comunicações ou perturbação do funcionamento de sistemas informáticos. Temos então que pensar que a Internet contém riscos, mas a vida fora da Internet também os tem.

3. A filtragem de conteúdos

Com a filtragem de conteúdos pretende-se impedir o acesso de alguns ou de todos os elementos de uma comunidade escolar a determinados assuntos. Isto levanta algumas questões. Desde logo, seria o filtro igual para todos ou teriam os professores, funcionários e alunos permissões diferenciadas de acesso à Internet? Os alunos do 7.º ano têm permissões iguais aos alunos do 12.º? E quem decide os conteúdos a filtrar? Os filtros são eficazes?

O controlo pode ser feito a nível do país, a nível dos fornecedores do serviço, a nível institucional (empresas, escolas e cibercafés, por exemplo) e a nível local afectando apenas um computador (ONI – OpenNet Initiative, 2009). A Internet pode ser o único espaço de comunicação a nível global que é verdadeiramente livre, uma vez que os seus conteúdos não estão sujeitos a quaisquer critérios de selecção, editoriais, de marketing, políticos ou outros. Até nas bibliotecas, públicas ou privadas, existe alguma forma de controlo sobre o que está disponível para o público: em última instância alguém tem de escolher quais as obras a adquirir e quais as que estão de facto disponíveis.

A colocação de filtros, com vantagens e desvantagens, acaba com a liberdade de acesso à Internet num determinado espaço. Existe um factor que não deve ser negligenciado: os filtros muitas vezes filtram aquilo que não devem, com resultados absurdos (Bastian, 1997). Por exemplo, um site que lida com obras literárias pode ser bloqueado devido ao título Moby Dick, ou a um nome como Sussex. O próprio site do Ministério da Educação pode ser bloqueado por uma contagem demasiado alta da palavra oral. Se for decidido abordar a questão da educação sexual, por exemplo, o filtro irá

limitar fortemente os conteúdos. O mesmo pode acontecer, por exemplo, a jogos educativos se o filtro encontrar uma palavra que considera proibida (como, por exemplo a palavra «jogos»).

Também é necessário ressalvar que se um governo ou outra entidade declarar que os seus cidadãos (ou funcionários ou alunos, ou…) não podem ver conteúdos impróprios, pornográficos ou de violência extrema, tem logo à partida o problema de definir rigorosamente estes conceitos, o que não é pacífico. Um exemplo de diferença no entendimento de conceitos está no facto de uma mãe que colocou online uma foto em que aparecia a amamentar o seu filho ter visto a sua fotografia removida devido a uma queixa relacionada com a obscenidade da mesma (Collier, 2008).

Parece-nos que a aplicação dos filtros acarreta ainda o perigo de os pais e professores poderem pensar que têm o problema dos acessos indesejados resolvido e não gastarem tempo a conversar com os jovens, sendo estas conversas fundamentais. No que diz respeito à segurança na Internet, na melhor das hipóteses os filtros resolvem uma parte do problema, na pior dão uma falsa ideia de segurança (Linvingstone, 2001).

Além disso, se aplicarmos um filtro na escola, os jovens podem consultar a Internet num local livre de filtros, ou utilizar um aparelho sem filtro, como um telemóvel ou uma consola de jogos. Parece-nos que este assunto é bastante delicado, e haverá sempre opiniões diferentes da nossa, assim como haverá opiniões diferentes das de quem decide o que se pode ou não consultar. Os filtros são caracterizados por terem uma margem de erro que não é desprezável e, de qualquer forma, não substituem o esclarecimento dos utilizadores. Embora nos pareça que o que é ilegal deve, de facto, ser bloqueado, as coisas tornam-se menos claras quando falamos de conteúdos pornográficos, violentos, subversivos ou simplesmente inadequados, porque estes conceitos podem não ter os mesmos significados para todas as pessoas. Julgamos que os filtros a nível de escola não devem ser aplicados. Caso se decida pela aplicação pensamos que deve ser possível implementar uma política diferenciada entre os alunos e que deve ser possível aos encarregados de educação pronunciarem-se sobre o seu próprio educando, pedindo a aplicação ou não dos filtros, evitando uma política de bloqueio de conteúdos indiferenciada que afectaria todos os alunos de igual forma, sendo que a situação inicial para os alunos seria de não aplicação de qualquer filtro.

4. Metodologia

4.1. População e Amostra

O estudo desenvolveu-se no ano lectivo de 2008/2009 numa escola secundária com terceiro ciclo onde estudam 1075 alunos e trabalham 41 funcionários e 120 professores. O corpo docente é extremamente estável, sendo a quase totalidade pertencente ao quadro da escola. Da oferta formativa constam cursos vocacionados para o prosseguimento de estudos e cursos de carácter profissionalizante. Esta escola tem funcionado

fundamentalmente com cursos vocacionados para o prosseguimento de estudos, sendo que 90% dos alunos do ensino secundário e todos os alunos do ensino básico frequentavam este tipo de ensino. Também a divisão por níveis de ensino tem sido bastante assimétrica, verificando-se que 72% dos alunos frequenta o ensino secundário enquanto apenas 28% frequenta o ensino básico. Dos 1075 alunos, 45,5% são rapazes e 54,5% são raparigas e têm idades compreendidas entre os 12 e os 19 anos.

Foi preferida a utilização de questionários como instrumento de recolha de dados, pois interessou saber quais os números reais relativos aos comportamentos dos alunos utilizadores da Internet. Pretendeu-se saber quantos alunos praticavam determinadas actividades enquanto utilizadores da Internet, de modo a aferir onde deve ser focada maior atenção no projecto a desenvolver. Interessava fundamentalmente quantificar os casos, obter uma visão global da realidade e posteriormente tirar conclusões e agir. Segundo Quivy & Campenhoudt (1998) o método de recolha de informações por questionário é especialmente adequado para casos em que é necessário interrogar um grande número de pessoas e garantir um maior anonimato.

Foi realizado um pré-teste para o questionário aplicado aos alunos, envolvendo duas turmas: uma do sétimo ano e outra do décimo. Escolheu-se uma turma do sétimo ano porque se pensava que estes alunos, sendo os mais novos, apresentassem maiores dúvidas e necessitassem de mais tempo para responder ao questionário do que os restantes. Escolheu-se também uma turma do décimo ano para obter as reacções de alunos do secundário Os questionários foram aplicados em sala de aula e em suporte electrónico. Os pré-testes não revelaram falhas para além de um ou outro erro ortográfico, como por exemplo a palavra particar em vez de praticar.

Após a realização do respectivo pré-teste considerou-se que se devia aplicar o questionário destinado aos alunos de forma a obter uma amostra representativa e significativa. Para obter a amostra, seleccionaram-se três turmas do ensino básico, sendo uma de cada ano. Seleccionaram-se também três turmas do 10º ano e outras três turmas do 11º. Para o 12º ano seleccionaram-se duas turmas, uma vez que o número de alunos deste nível é inferior ao apresentado nos 10º e 11º anos.

O número total de respostas obtidas para análise (286) permite considerar que a amostra é representativa e significativa (cf. Almeida & Freire, 2007).

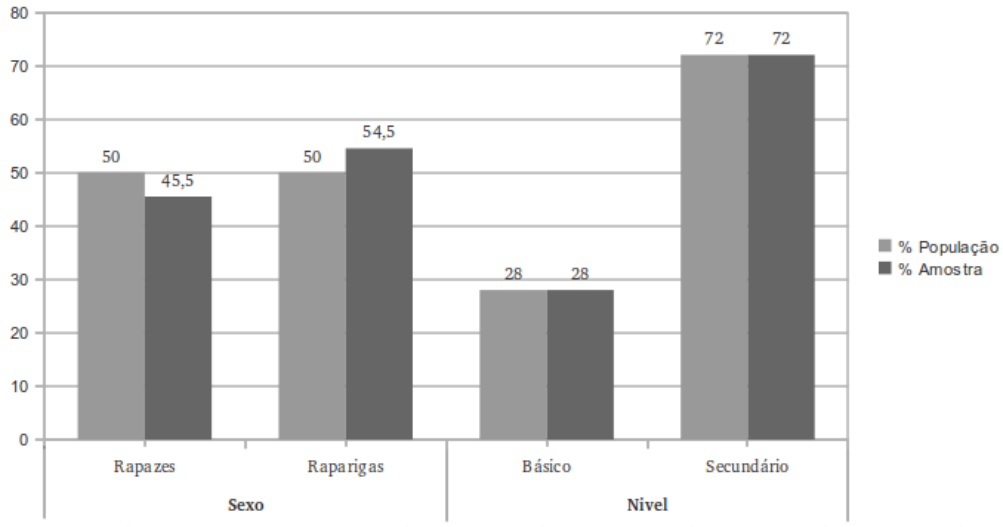

Gráfico 1. Comparação entre a amostra e a população para o sexo e o nível de ensino dos alunos

Conforme a gráfico 1, verifica-se que a amostra é semelhante à população. A população é composta por 45,5% de rapazes e 54,5% de raparigas enquanto que a amostra é constituída por 50% de rapazes e raparigas. A amostra e a população são iguais na percentagem de alunos por nível de ensino, sendo 28% destes alunos do ensino básico e 72% alunos do ensino secundário. Para os questionários aplicados aos encarregados de educação e aos professores não foi realizado nenhum préteste tendo, no entanto, sido mostrados os questionários a dois professores e a dois encarregados de educação de forma a procurar corrigir alguns pontos que não estivessem claros para os participantes. Nestes não foram reveladas falhas.

Foi possível obter 256 respostas de encarregados de educação. Conforme se pode verificar pela análise da gráfico 2, a população e a amostra são semelhantes no que diz respeito às habilitações literárias. A comparação é feita por este parâmetro porque, dos dados preenchidos no questionário este é o único que tem dados consistentes no programa informático de gestão de alunos. Tal não acontece por género ou idade, por exemplo. Esta amostra foi obtida pedindo aos encarregados de educação dos alunos que responderam aos questionários para preencherem, eles próprios, o questionário respectivo. Como o número de respostas devolvidas não era suficiente foi pedida a colaboração dos encarregados de educação aquando das matrículas. Obteve-se, assim, um total de 256 respostas por parte dos Encarregados de Educação, número que fica um pouco aquém do desejado, uma vez que para um intervalo de confiança inferior a 5% com um nível de confiança de 95% o número de respostas deveria ser de aproximadamente 280 (cf. Almeida & Freire, 2007).

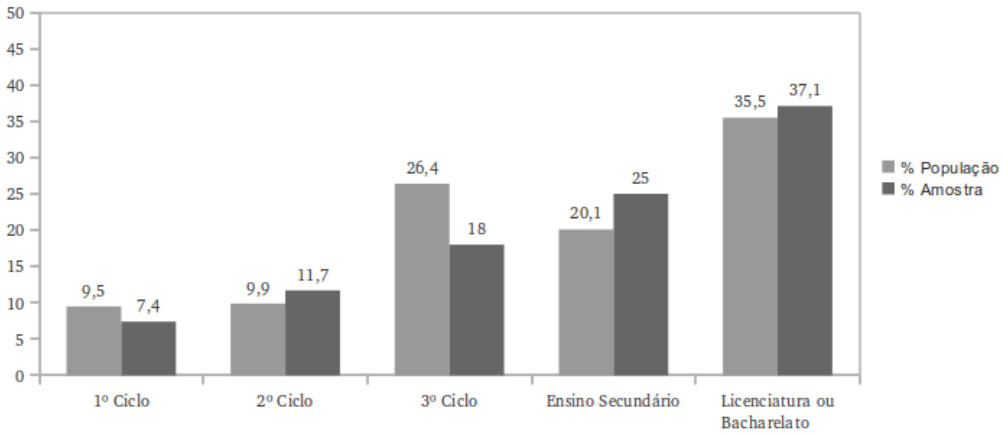

Gráfico 2. Comparação entre amostra e população por habilitações literárias relativamente aos encarregados de educação.

Relativamente aos professores, o processo foi mais simples: pediu-se a colaboração de todos. No entanto, apenas 95 professores responderam aos questionários, correspondendo a 79,1%, do total de professores da escola, o que representa uma amostra significativa (cf. Almeida & Freire, 2007).

4.2. Instrumentos de Recolha de Dados

Dos estudos analisados considerou-se que o Survey of Internet and At-Risk Behaviors conduzido por Samuel McQuade III em 2008 se mostrava como o mais adequado e semelhante ao que se pretendia concretizar. Os questionários que serviram de base aos utilizados neste estudo estão publicados na Internet no endereço http://www.rrcsei.org/research.html, tendo sido concedida a autorização para os adaptar e utilizar.

Estes questionários foram traduzidos da língua inglesa e adaptados para a implementação deste estudo. Este processo foi executado com o objectivo de conseguir uma tradução fiel ao original. As adaptações circunscreveram-se à simplificação e redução do número de questões e também à adaptação à realidade do estudo, uma vez que os questionários originais se destinavam a várias escolas nos Estados Unidos e não a uma única escola portuguesa.

O questionário para os alunos foi aplicado online. Este questionário foi elaborado de forma a não permitir respostas em branco. As questões foram todas consideradas obrigatórias, não sendo possível submeter o questionário no caso de existir alguma resposta em falta. No entanto, quando uma questão dependia da resposta anterior, ela só era mostrada se tal fosse necessário. Por exemplo, a questão onde se pergunta «qual foi o problema pessoal causado pela utilização da Internet» (a última questão do questionário aos alunos) só é mostrada caso se tenha respondido Sim na questão anterior, e neste caso a resposta será obrigatória.

Os resultados obtidos nalgumas questões (n=31) deste questionário aos alunos1 foram sujeitos a uma primeira análise factorial exploratória em

componentes principais com rotação varimax (KMO = 0.810 ≈ 0.8; χ^2=7379,239 , p < 0.001), realizado com o software SPSS v. 17. (ver quadro 1). Foi possível, nesta primeira análise, identificar cinco factores com alfas de Cronbach aceitáveis:

- O primeiro factor, que se relaciona com acessos não autorizados, corrupção de sistemas, e vendas de trabalhos de casa, obteve um valor para o Alfa de Cronbach de 0,910. Denominamo-lo como "Hacking/Cracking e compra de projectos escolares" e é composto por 9 itens;
- O segundo factor, que se relaciona com o sexo e a pornografia, o valor obtido para o Alfa de Cronbach foi de 0,881. Denominámos este factor como "Utilização relacionada com sexo e pornografia" e é composto por 7 itens;
- O terceiro factor, que se relaciona com a utilização fraudulenta de cartões de crédito na Internet, o valor obtido para o Alfa de Cronbach foi de 0,804. Apelidamos este factor de "Utilização para obter lucro ilícito" e é composto por 3 itens;
- O quarto factor emergente, relacionado com o engano do outro, com ameaças a outros e ainda com conversas sobre sexo, o valor obtido para o Alfa de Cronbach foi de 0,720. Chamámos este factor como "Utilização para enganar e incomodar outros" e é composto por 5 itens;

Finalmente o quinto factor, que se relaciona com as fraudes em testes e exames, o valor obtido para o Alfa de Cronbach foi de 0,543. Designámos este factor como "Fraude em testes e exames" e é composto por 2 itens. Embora não tenha o número de itens mínimo para se poder considerar como um factor (e que alguns autores consideram ser 3, cf. Marôco, 2007) mantivémo-lo pois integra comportamentos fraudulentos que nos parecem importantes e que, num estudo psicométrico posterior, se poderá melhorar integrando novos itens.

Emergiu um sexto factor, que obteve um Alfa de Cronbach de 0,314, que considerámos inaceitável e por isso foi eliminado. O valor do Alfa de Cronbach para o conjunto de todas as questões (31) que compõem os 6 factores que emergiram da análise factorial é de 0,920, o que pode ser considerado muito bom. Estas questões relacionam-se com a agressividade, o engano, a fraude e a delinquência, tudo comportamentos de risco, que são praticados por alguns jovens inquiridos quando usam a Internet e outros serviços online.

Para o questionário aos professores seguiu-se o mesmo processo. Obteve-se um KMO =0.741≈ 0.7 e um χ^2=150,263, p-value < 0.001. Emergiram 2 factores, mas só 1 com um valor de Alfa de Cronbach aceitável ou mesmo bom (α= 0,780). Os 5 itens que integram este factor estão relacionados com os conhecimentos do professor sobre a Internet e os perigos que lhe estão associados. Relativamente ao questionário aos pais

não foi possível fazer a análise factorial devido ao resultado do teste KMO ser inferior a 0,7 (pressuposto essencial para se aplicar este tipo de análise).

N.º Questão	Descrição Questão	Componente							
		1	2	3	4	5	6	7	8
24-5	Browsing em sistema	,877	,083	,109	,035	,161	-,117	,039	,141
24-2	Corromper sistema	,844	,087	,186	,086	-,008	,325	,000	,064
24-1	Revelar falhas	,786	,060	,116	,066	,058	,338	-,132	,033
24-6	Alterar ficheiros	,761	,212	-,095	,123	,257	,193	,218	-,111
24-7	Aceder usando malware	,750	,258	,368	,090	,136	-,059	,149	,119
24-4	Descobrir senha	,629	,175	,167	,140	,184	,112	-,132	,378
24-8	Contornar filtro	,566	,158	,369	,111	,084	-,108	,017	-,016
24-3	Escrever soft malicioso	,513	,404	,499	,049	,037	-,093	,327	,085
23-2	Comprar trabalhos de casa	,484	,341	,069	,172	,257	,433	,185	-,157
21-3	Download porno	,031	,838	,015	-,021	,240	,145	-,162	,109
21-5	Download porno de mais velhos	,107	,827	,028	,026	,292	,148	-,081	,156
21-1	Enviar pornografia	,343	,753	,164	,084	-,069	-,080	,027	,182
21-4	Download porno jovens	,164	,705	,330	,351	,011	,028	,161	-,081
21-2	Enviar pornografia de ti	,098	,700	,243	,317	-,161	,127	,127	-,193
21-6	Publicar porno de ti	,143	,594	,439	,416	-,021	,118	,134	-,231
20-4	Pedir para fazer sexo	,338	,548	,077	,246	-,132	-,081	,144	,205
22-1	Obter o número de cart cred	,205	,186	,894	,004	-,013	,142	-,045	,032
22-2	Utilizar o num cart cred	,237	,193	,878	,113	,063	,208	,016	-,016
23-3	Vender trabalhos de casa	,287	,068	,488	,196	,311	,216	,307	,024
20-2	Mentir acerca do sexo ou aspecto	,026	,124	-,047	,830	,123	-,017	-,002	-,006
20-3	Pedir para falar de sexo	,157	,331	,018	,680	-,062	,064	,108	,100
20-1	Mentir acerca da idade	,068	-,055	,172	,609	,124	,145	-,136	,296
19-5	Ameaçar outro	,137	,317	,203	,581	,105	,254	,192	-,119
19-4	Publicar inf embaraçosas	,170	,056	,114	,473	,371	,190	,378	-,199
23-4	Copiar nos testes	,142	,109	,022	,021	,779	,014	,022	,141
23-5	Copiar nos exames	,272	-,020	,072	,216	,645	-,037	,197	-,065
	Enviar spam	,142	,077	,254	,149	-,078	,760	,082	,117
	Cometer plágio	,143	,146	,288	,242	,270	,388	,063	,042
	Usar conta de outro	,000	,004	,044	,052	,143	,088	,839	,124
19-1	Fornecer password	,239	,126	-,214	-,084	-,082	,360	,192	,665
19-3	Incomodar outro	,122	,160	,206	,376	,236	-,144	,076	,599

Quadro 1. Resultado da Análise Factorial em Componentes Principais: Matriz de Componentes Rodada (Rotação Varimax).

4.3. Questionários Online

O questionário foi instalado num computador portátil pessoal, que serviu de servidor. O sistema operativo utilizado foi o *Ubuntu* 8.04 e a ferramenta de criação de questionários foi o *LimeSurvey* 1.72. O número de respostas foi controlado à entrada e à saída de cada grupo para haver a certeza de que o número de respostas obtidas correspondia ao número de alunos que efectivamente responderam.

5. Resultados

Relativamente aos alunos destacam-se os seguintes resultados, reportados apenas aos últimos 12 meses de utilização da Internet, tendo os questionários sido aplicados entre Março e Abril de 2009.

5.1. Hábitos de Utilização

Cerca de 35 por cento (37,4%) dos alunos aprenderam sozinhos a utilizar o computador; 24,2% indicaram que a pessoa com quem aprenderam mais foi com um irmão ou irmã; 15,4% indicaram os pais e 12,2% referiram um amigo ou amiga. Apenas 6,6% nomeiam um professor e 4,2% indicaram "outro". Os dispositivos utilizados no acesso à Internet são em 87% dos caso o computador portátil, seguindo-se o computador de secretária (85%), o telemóvel (39%) e a consola de jogos regular (18%) e portátil (15%). O PDA é referido por 9% dos alunos e o i-pod por 4,2 por cento. A idade média de iniciação na utilização de computadores é aos 9 anos e o tempo médio gasto online por semana é de 12,5 horas. As actividades online são praticadas quase sempre em casa e 72% dos estudantes afirmou que o grau de supervisão parental era "nenhuma" ou "pouca", contrariamente ao que referem os encarregados de educação (ver gráfico 3).

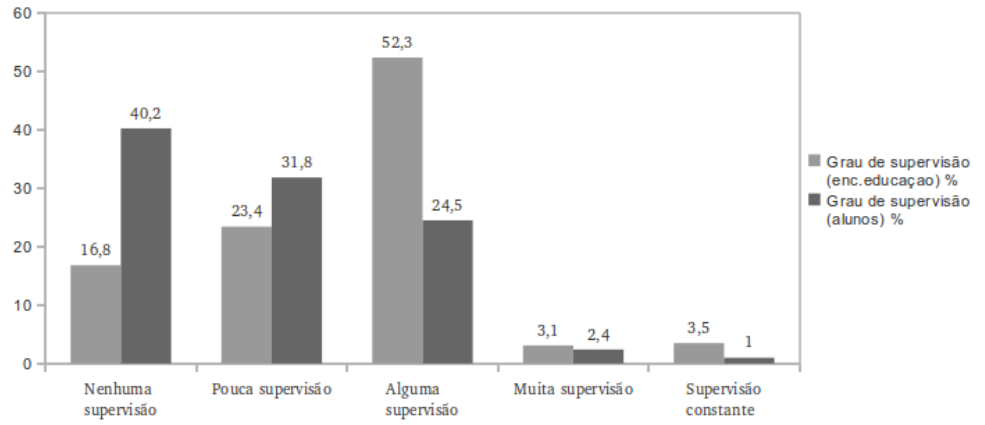

Gráfico 3. Grau de supervisão (comparação entre respostas de alunos e encarregados de educação).

Apenas 27,3% dos alunos referiram ter um limite de tempo para aceder à Internet enquanto 52,3% dos encarregados de educação afirmaram limitar o tempo disponível para o acesso à Internet por parte dos seus educandos, conforme a figura 4. Neste caso houve aproximadamente 2,4% de respostas inválidas.

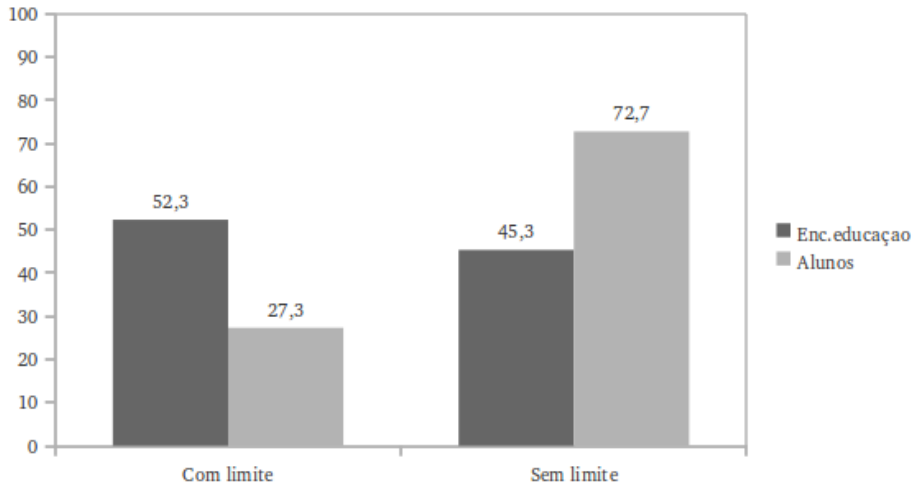

Gráfico 4. Limite de tempo (comparação entre respostas de alunos e encarregados de educação).

5.2. Comportamentos com Potencial de Risco e Vitimização

Nesta categoria incluímos alguns comportamentos praticados pelos jovens inquiridos que, na sua aparente normalidade, podem acarretar riscos para os alunos. Cerca de 60% dos estudantes inquiridos fala online em salas de conversação ou chats rooms, sendo que 57% utiliza a Internet para falar de assuntos íntimos e dentre estes 2,4% (7 alunos) já falou com estranhos sobre estes assuntos. 42% dos alunos utiliza a Internet para namoriscar e 36,4% para discutir o seu aspecto físico, sendo que 3,5% com estranhos.

Cerca de 24% dos inquiridos já conversaram na Internet sobre sexo, 12,6% foram questionados acerca dos seus hábitos sexuais e 13,3% viu pornografia acidentalmente. A 14,7% dos inquiridos foi pedido um encontro em pessoa; 10,1% seguiram conselhos dados via Internet, sendo que 5,2% aceitaram encontrar-se com um desconhecido e 6,6% pediram encontro a um desconhecido; 1,7% afirmou ter dado informações pessoais online a desconhecidos. Deve-se reter ainda que 20,3% mentiu acerca da idade e 5,6% acerca do sexo ou aparência, o que se configura como engano do outro, o que se enquadra no factor 4 que se denomina "Utilização para enganar e incomodar outro".

Nos comportamentos de vitimização incluímos o uso da Internet que levou a situações nas quais o aluno foi incomodado, chantageado ou perseguido por alguém. Temos assim que: 16,4% dos estudantes (47 numa amostra de 286) afirmaram que alguém já utilizou a Internet para os incomodar; 9,4% que foi vítima de acesso remoto não autorizado ao seu computador; 4,9% (14 alunos) afirmaram que alguém utilizou a Internet para os chantagear; 3,5% para lhe roubar algo; e 1,7% disseram que alguém utilizou a Internet para os perseguir. Alguns destes comportamentos podem ser incluídos na categoria do cyber-bullying, isto é, alguns estudantes por nós inquiridos foram sujeitos no ano lectivo de 2008/2009 (altura em que foram recolhidos os dados) a pressões, chantagens e perseguições feitas via Internet, sendo alguns destes comportamentos feitos pelos seus pares.

5.3. Comportamentos com Potencial de Risco, Ilegais e de Delinquência

Nesta categoria incluímos os itens que compõem os factores «Hacking/Cracking e compra de projectos escolares», «Utilização para obter lucro ilícito» e «Fraude em testes e exames». Verificou-se que 63,3% dos jovens inquiridos afirmaram ter feito downloads ilegais de música e/ou filmes e 57% referiram ter feito downloads ilegais de software. Estes valores confirmam que o acesso a materiais protegidos por direitos de autor é praticado por um elevado número de alunos, levantando-se as questões: como se deve combater este hábito? E deve-se punir? Em caso afirmativo, como?

Relativamente aos conteúdos, 10,1% dos alunos referiram ter acedido a sites que incitam à violência e 4,5% disseram ter acedido a sites que incentivam o racismo. Estes sites, pelos seus conteúdos, podem conduzir os alunos a ter comportamentos ilegais e perigosos.

Relativamente à filtragem de conteúdos, verifica-se que 7% dos alunos inquiridos referiram já ter contornado um filtro de conteúdos, o que representa 17,7% dos alunos que utilizam computadores equipados com filtro. Se a esta informação juntarmos o facto de 47% dos alunos que utilizam computadores equipados com filtros de conteúdos também utilizarem outro dispositivo para aceder à Internet ficamos com algumas questões importantes para resolver: qual o grau de importância e de confiança da filtragem? Serão os benefícios da filtragem superiores aos transtornos causados pela própria filtragem?

Relativamente ao acesso a informações confidenciais sem autorização, verificou-se que 12,6% dos alunos inquiridos admitiram já ter adivinhado ou forçado a descoberta de uma password, 1,7% já recorreu a um computador para utilizar ilegalmente o número de cartão de crédito de uma pessoa, enquanto 1% já utilizou a Internet para descobrir o número de cartão de crédito de outra pessoa; 7,7% dos alunos inquiridos referiram já ter acedido a sistemas de outras pessoas sem autorização, 4,9% admitiram já ter alterado ou eliminado ficheiro num sistema de outra pessoa, sem permissão, 6,3% assinalaram já ter corrompido/atacado um sistema informático, 5,9% admitiram já ter criado software malicioso, 4,9% já deram a password de um colega a outra pessoa sem consentimento, cerca de 5,6% já utilizaram a password de um colega sem consentimento. Este tipo de comportamento é ilegal e pode causar problemas graves a quem o pratica. Além disso estes actos são eticamente condenáveis e merecedores de uma intervenção por parte da escola.

No que diz respeito à fraude escolar, verificou-se que 5,2% dos inquiridos já utilizaram a Internet para comprar projectos escolares e 4,2% utilizaram a Internet para os vender; verificou-se ainda que 5,2% dos jovens inquiridos admitiram já ter cometido plágio enquanto 13,3% já utilizou um dispositivo electrónico para copiar em testes e 4,2% já utilizaram um dispositivo electrónico para copiar em exames. Uma vez que apenas os alunos dos 9.º, 11.º e 12º são sujeitos a exames podemos concluir que, possivelmente, a percentagem de alunos sujeitos a exame que copia utilizando dispositivos electrónicos é superior. Os valores relativos à fraude escolar não são desprezáveis, justificando-se uma acção de sensibilização sobre esta matéria.

Deve-se ainda registar que 7% dos inquiridos afirmaram ter jogado a dinheiro online, sendo este número merecedor de atenção. Por último devemos registar que 19,6% referiram ter acedido a pornografia online; este tipo de comportamento é merecedor de atenção, uma vez que os sites pornográficos são muitas vezes agressivos na sua programação, tentando aproveitar falhas de segurança nos computadores e instalando vírus. Além disso muitas vezes são propostos contactos em pessoa e o acesso a conteúdos pagos.

Relativamente aos professores destacam-se os seguintes resultados: Verificou-se que 61,1% indicaram que sabem menos ou muito menos do que os seus alunos. Relativamente à utilização dos computadores, 35,1% classificam o seu nível de confiança para supervisionar os seus estudantes como “nenhuma confiança” ou “pouca confiança” e 24,2% classifica o seu nível de conhecimentos relativamente aos perigos da Internet como “inexistentes” ou “muito fracos”, enquanto que 49,5% classifica-os como “médios” e apenas 26,4% como “bons” ou “muito bons”; Estes valores sugerem que os professores não estão prontos a responder com segurança a possíveis questões levantadas pelos alunos. Relativamente à abordagem destes assuntos na sala de aula verifica-se que 15,8% dos professores não fala com os seus educandos sobre os riscos na utilização da Internet enquanto 31,6% raramente aborda este tema.

Relativamente aos encarregados de educação destacam-se os seguintes resultados: As respostas relativas ao nível de supervisão mostram valores muito diferentes dos indicados pelos alunos, conforme a gráfico 3. O mesmo se passa relativamente ao limite de tempo para aceder à Internet: apenas 27,3% dos alunos afirmaram haver um limite de tempo enquanto 52,3% dos encarregados de educação afirmaram existir esse limite, conforme a gráfico 4. Registou-se ainda que 39,9% dos encarregados de educação verificam os sites visitados pelos seus educandos menos de uma vez por mês ou não verificam de todo; Por outro lado, 13,9% dos encarregados de educação referem que raramente ou nunca conversam com os filhos sobre a utilização da Internet. Estes resultados sugerem que os encarregados de educação muitas vezes não sabem, de facto, quais os hábitos de utilização da Internet por parte dos seus educandos.

6. Conclusões

A análise dos resultados obtidos permite concluir que todos os comportamentos incluídos nos questionários são praticados por alguns alunos. Deste facto resulta a necessidade de intervir sobre uma grande variedade de comportamentos, tornando-se imperioso atribuir a cada tópico seleccionado uma fatia de tempo adequada à sua pertinência, possíveis consequências e quantidade de alunos que o praticam. Destacam-se os comportamentos associados ao racismo e violência, a encontros com desconhecidos, a fraudes com cartões de crédito, a acessos indevidos a sistemas informáticos, à utilização da Internet para incomodar de alguma forma outras pessoas, ao plágio e a fraudes em testes e exames. Os downloads ilegais são também praticados por um número elevado de alunos, mas este não é de todo um facto surpreendente, uma vez que são muitas as notícias que dão conta de números elevados de pirataria, não só no nosso país mas também no estrangeiro. A questão dos encontros com desconhecidos também merece atenção, bem como os conteúdos que são colocados online pelos alunos.

Verifica-se igualmente que os comportamentos indicados nos questionários são quase sempre praticados em casa, sendo muito reduzido o peso dos comportamentos praticados na escola ou noutro local. Este é um dado importante que remete para o tema das conversas que se devem ter com os alunos e também para o tema da filtragem de conteúdos. Se aplicamos filtros nas escolas limitamos o acesso para todos, mas normalmente as actividades online são praticadas em casa. Serão os benefícios superiores aos transtornos causados?

Destacam-se ainda os números divergentes entre alunos e encarregado de educação no que respeita a limites de tempo e supervisão. Estes valores sugerem que os hábitos de utilização da Internet por parte dos educandos não são, muitas vezes, claros para os encarregados de educação.

Uma vez que a maioria dos professores (61,1%) considera que sabe menos ou muito menos que os seus alunos relativamente a este tema, verificamos que existe um vazio de conhecimentos que importa preencher,

de forma a proporcionar aos jovens maiores oportunidades de esclarecimento de dúvidas relativemente a este tema. A escola pode desempenhar um papel fundamental nesta matéria, uma vez que por ela passam todos os jovens do nosso país.

Em suma, a área da educação e formação para a utilização da Internet merece, de facto, uma intervenção e julgamos que este tema deveria passar a fazer parte das competências dos professores de hoje. As escolas deveriam igualmente pensar em programas de intervenção nesta área, destinados a professores, alunos e pais, sobretudo numa abordagem preventiva.

7. Referências bibliográficas

Almeida, L. S., & Freire, T. (2007). *Metodologia da investigação em psicologia e educação* (4.ª ed.). Braga: Psiquilíbrios Edições.

Bastian, J. A. (1997). *Filtering the internet in american public libraries: sliding down the slipery slope*. First Monday. Retirado em 29 de Dezembro de2008, de http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/557/478

BES. (2009). *Lista dos ataques mais recentes*. Retirado em 9 de Julho de 2009, de http://www.bes.pt/sitebes/cms.aspx?plg=8a7c1302-08a7-426d-95e9-4d475f1ff431

Collier, Anne. (2008). *Breastfeeders protest Facebook's terms.* Retirado em 28 de Março de 2010 de http://www.netfamilynews.org/2008/12/breastfeeders-protest-facebooks-terms.html

Comissão Europeia. (2008). *Safety tips*. Retirado em 31 de Dezembro de 2008, de http://ec.europa.eu/information_society/activities/sip/safety_tips/index_en.htm

Livingstone, S. (2001). *Online freedom & safety for children*. Retirado em 31 de Dezembro de 2008 de http://www.infoamerica.org/documentos_pdf/livingstone06.pdf

Maroco, J. (2007). *Análise estatística com a utilização do SPSS* (3ª ed.). Lisboa: Edições Sílabo, Lda

McQuade, S. C., & Sampat, N. (2008). *Survey of internet and at-risk behaviors*. retirado em 28 de Dezembro de 2008, de http://www.rrcsei.org/RIT%20Cyber%20Survey%20Final%20Report.pdf

Microsoft. (2010). *O essencial sobre segurança.* Retirado em 28 de Março de 2010 de http://www.microsoft.com/portugal/athome/security/protect/windowsxp/Default.mspx.

Ministério da Educação. (2007). *Plano tecnológico da educação*. Retirado em 24 de Janeiro de 2009, de http://www.escola.gov.pt/docs/me_plano_tecnologico_educacao.pdf

Oliveira, W. (2000). *Técnicas para hackers: Soluções para segurança*. Lisboa: CentroAtlântico.

OpenNet Initiative. (2009). *About filtering*. Retirado em 29 de Janeiro de 2009, de http://opennet.net/about-filtering

Papert, S. (1996). *A Família em rede (5.ª ed.)*. Lisboa: Relógio D'Água.

Ponte, C. (2008). *Crianças e Internet: oportunidades e riscos*. Retirado em 21 de Dezembro de 2008 de http://inquietacaopedagogica.blogspot.com/2008/09/crianas-e-internet.html

Ponte, C., & Vieira, N. (2008). *Crianças e Internet, riscos e oportunidades - um desafio para a agenda de pesquisa nacional*. Retirado em 27 de Novembro de 2008, de http://www2.fcsh.unl.pt/eukidsonline/docs/EU_Kids_OnlineVersao170707.pdf

Quivy, R., & Campenhoudt, L. V. (1998). *Manual de investigação em ciências sociais*. Lisboa: Gradiva.

Ribeiro, A. T., & Rosa, C. M. S. *A Internet e os direitos de autor*. Retirado em 1 de Janeiro de 2009, de wiki.di.uminho.pt/twiki/pub/Education/Archive/InformaticaJuridicaT25/CasimiroRosaAbilioRibeiro1.doc

Santander-Totta.(2008). *Segurança*. Retirado em 30 de Dezembro de 2008, de http://www.santandertotta.pt/pagina/indice/0,,680_1_1,00.html

Silva, L., & Remoaldo, P. (1997). *Introdução à Internet (3.ª ed.)*. Lisboa: Editorial Presença.

Turkle, S. (1995). *A Vida no ecrã*. Lisboa: Relógio D'Água Editores.

Wolak, J., Mitchell, K., & Finkelhor, D. (2006). *Online victimization of youth: five years later*. Retirado em 28 de Dezembro de 2006, de http://www.unh.edu/ccrc/pdf/CV138.pdf

Wolak, J., Finkelhor, D., Mitchell, K. J., & Ybarra, M. L. (2008). Online predators and their victims - myths, realities, and implications for prevention and treatment. *American Psychologist*, 63, 111-128. Retirado em 28 de Março de 2010 de http://www.unh.edu/ccrc/pdf/Am%20Psy%202-08.pdf