CYBERLAW

by CIJIC

CYBERLAW

by CIJIC

CYBERLAW

by CIJIC

EDIÇÃO N.º IV – SETEMBRO DE 2017

REVISTA CIENTÍFICA SOBRE CYBERLAW DO CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO – CIJIC – DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

CYBERLAW by CIJIC

CIJIC: CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

ISSN 2183-729

NOTAS DO EDITOR:

O presente número assume a responsabilidade de procurar encontrar algumas respostas à questão prejudicial: *«Como proteger crianças e jovens, adultos e séniores, neste universo, "paralelo", virtual, de imigrantes e nativos digitais?»*.

Hodiernamente, o "***digital***" instalou-se no quotidiano da maioria das pessoas, fazendo parte integrante da nossa nova forma de interacção social. É na economia, finanças, saúde, ensino, Governo, participação cívica, cultural, sociológica… enfim, o mundo! Há todo um novo palco para desenvolvermos aquelas nossas acções típicas, humanas, num outro paradigma, o do digital. Uma ***avatarização***, multifeixe, em que o Homem transcende-se a uma sua natural condição de uno, indivisível, irrepetível, no mundo terreno, abraçando múltiplos actores, e papéis, no mundo digital.
O apego desta transcendência digital – *quási-divina* -, se, por um lado, nos permite ultrapassar limitações físicas naturais e nos transporta para presenças e ofícios simultâneos, multiponto e multitarefa, por outro lado, como qualquer outro apego, apresenta a virtualidade (em alguns casos já, real) de nos transformar em escravos-de-modernidade, onde o paradigma "**tecnologia ao serviço do Homem**" é suplantado pela dinâmica disruptiva do momentum digital – e de certa práxis -, pelo seu inverso, i.e., "*Homem ao exclusivo da tecnologia*".

Não obstante, julgamos não ser o momento para adotarmos uma cultura e atitude temerárias. Se há característica humana que nos distingue é a inteligência. Singular, é ela

que nos conduz(iu) à criação de todo aquele cardápio de ferramentas que têm acompanhado, paralelamente, a nossa milenar evolução enquanto espécie ciente e consciente. E o mundo digital é apenas e só uma ferramenta. Outra. Nova. Mas uma ferramenta. Mantenhamos o consciente no radical "**tecnologia ao serviço do Homem**" e o ciente permitir-nos-á conviver de forma harmoniosa com tal ferramenta, auxiliar às nossas intrínsecas limitações e insatisfações humanas. Ademais, é toda esta procura de um "*completar e satisfazer as nossas incapacidades e insatisfações*" que nos vai lançando na prossecução de um contínuo melhorar do bem-estar comum e nos vai fazendo evoluir ao longo dos tempos.

O tema, recuperando, praticamente em exclusivo, desta nova edição da "Ciberlaw by CIJIC", procurará desmistificar alguns dos problemas, recorrentes, associados ao "*mundo digital*": a cultura educacional *online*. Reconhecendo, aprioristicamente, o espaço – com uma margem já considerável de consolidação – de actuação jurídica *online*, quer mundial, quer europeu, quer nacional – ao qual voltaremos em futuras publicações – assumimos o desafio de, nesta edição, destacar a tónica sobre a pessoa, mais juvenil, e de certa forma também todos os outros, e o modo com esta se relaciona neste *novo mundo*, acentuando comportamentos que acabamos por assumir *online*, com ou sem conhecimento dos impactos daí derivados ou deriváveis.

Partindo da premissa lançada em 2001 por Mark PRENSKY, «*Digital Natives, Digital Immigrants*», a ferramenta digital denota uma particularidade, prontamente, assinalável: qual Ágora do Séc.XXI, encontramos uma confluência, massiva em alguns casos, neste palco, de gerações de pessoas tão diferentes quanto *baby boomers*, *millenials*, *post-millenials* ou *iGen*. Nesta multitude de pares em palco(s) comum(ns), colidimos com "tais" imigrantes e "tais" nativos digitais ao virar de cada página, a cada clique que concedemos. Se os primeiros nasceram e cresceram num outro tempo com outras ferramentas, é inegável que também foram eles que deram os passos para o desenvolvimento desta nova ferramenta digital; se muitos outros deles se depararam na contingência de a ela se adaptarem, aqueles nascidos já neste tempo, *de modernidade*, parecem denotar um conhecimento tecnológico *"genético"*, natural, que apenas releva um dado *momentum* digital: o presente.

Seja qual a forma em que qualquer uma de todas estas gerações de humanos se encontre no digital, é, ainda assim, imperioso notar que a literacia digital não encontra, necessariamente, uma correspondência com a factualidade da tal "*separação*" de Prensky. Nem dos cliques. Se há um factor constante, contínuo, cíclico, na generalidade de diversos dos problemas digitais associados às mais díspares formas de agressão *online* (sejam ciberataques; roubo de bases de dados; infecções virais mundiais; bloqueios de infraestruturas críticas; etc..), esse factor, é, sem rodeios, **o factor humano**.

A título de exemplo, notemos algumas singularidades: os *imigrantes digitais*, compelidos pela pulsão actual, procuram adaptar-se à novidade com a resiliência que lhes possa ser possível. Mais das vezes, através de um *autodidatismo* – perigoso - ignoram quer os riscos, quer as potencialidades. Uma combinação deveras "*penosa*", cujas más experiências *online* os excluirão do digital. Por outro lado, os *nativos digitais*, pela facilidade, em muitos dos casos, derivado de um tal "*dom temporal*", mas também pela falta de literacia e de conhecimento, ao negligenciarem – até pela imaturidade típica da sua juventude – os riscos em que podem incorrer, tornam-se, por excelência, num alvo preferencial das mais variadas formas de agressão digitais. Em movimento semelhante à dos *imigrantes digitais*, a colecção de más experiências, acabará por redundar numa exclusão digital.

É, por tanto, pungente, firme, a necessidade de reformatação da forma de protecção a conferir às pessoas que, avatarizando a sua presença no contexto digital, muitas das vezes se encontram completamente sozinhas, esvaziadas quer de instrumentos/ferramentas quer de conhecimento, nas mais variadas interacções praticadas *online*. Como no mundo real, a educação é o caminho. Que deveremos trilhar. Incessantemente.

Seja qual for a resposta possível a algumas das interjeições em curso, entendemos que se a pretensão passa por continuar a migração digital das nossas acções mundanas – com confiança e em segurança, possíveis - mais do que desejarmos ter um ***polícia-digital*** ao virar de cada clique, é imprescindível conferir competências educacionais, básicas, mínimas, digitais, a todos e a cada um de nós. O foco incide, por agora, sobre a

cibereducação. Só uma compreensão, mínima, deste *novo mundo digital*, só um conhecimento precípuo das suas potencialidades e riscos, nos permitirá trilhar o registo mais abrangente – que desejavelmente quereremos – e por tal, inevitavelmente, mais inclusivo, de todos, neste contexto. Que se instalou entre nós para ficar. E assim permanecerá connosco por muitos dos vindouros anos.

Saibamos, pois, aproveitar as oportunidades. Estejamos preparados para as agarrar.

Procuramos lançar um repto à comunidade para que se pronunciasse sobre o tema «Como proteger crianças e jovens, adultos e séniores, neste universo, "paralelo", virtual, de imigrantes e nativos digitais?».

O resultado é este.

Cabe-nos tão-só a honra de o apresentar.

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente*.**

Boas leituras.

Lisboa, FDUL, Agosto/Setembro de 2017

Nuno Teixeira Castro

ÍNDICE

DOUTRINA

CIBEREDUCAÇÃO COMO MEDIDA PREVENTIVA NO COMBATE AO CIBERCRIME

CYBEREDUCATION AS A PREVENTIVE MEASURE TO COMBAT CYBERCRIME

ANTÓNIO AUGUSTO RAMOS CARVALHO [1]

MÁRIO RUI MONTEIRO MARQUES [2]

1 Primeiro-tenente António Augusto Ramos Carvalho. Correio eletrónico: ramos.carvalho@marinha.pt
2 Capitão-tenente Mário Rui Monteiro Marques. Correio eletrónico: mario.monteiro.marques@marinha.pt

RESUMO

A invenção da internet foi uma das maiores descobertas tecnológicas da Humanidade, tendo provocado uma transformação profunda nos hábitos e estilos de vida em todo o mundo. Esta permitiu ter acesso à informação numa questão de segundos, podendo referir-se a título de exemplo, que em 2016 estiveram conectados através da internet 6,4 biliões de equipamentos eletrónicos em todo o mundo[3].

Porém, a utilização massiva da internet, se por um lado, oferece possibilidades de liberdade e democracia nunca antes vivenciados, por outro, potencia o desenvolvimento de formas ilícitas de utilização do ciberespaço.

Neste âmbito, o Cibercrime assume-se como um fenómeno que se encontra em elevado crescimento em todo mundo, onde o seu impacto vai muito além dos tradicionais danos económicos. Com efeito, verifica-se que os ciberataques colocam em risco a privacidade e a liberdade dos cidadãos, põem em causa a soberania do Estado, e podem ainda divulgar informação que ameace a segurança nacional.

Neste sentido, por forma a fundarem-se as bases essenciais para o combate eficaz ao cibercrime é absolutamente fulcral existir uma boa compreensão deste fenómeno criminoso que afeta tudo e todos. Por conseguinte, a cibereducação é a chave para o sucesso, sendo essencial colaborar-se para a consciencialização e ação política no que respeita à cibersegurança.

O presente artigo discute os desafios que o ciberespaço atualmente coloca a todos os setores da nossa sociedade, sobretudo devido ao aumento generalizado do Cibercrime em todo o mundo, defendendo-se que a melhor estratégia de prevenção assenta no desenvolvimento de uma cultura de segurança da informação no ciberespaço, a qual somente será alcançada com a implementação de uma política de cibereducação na nossa sociedade.

Palavras-Chave: Cibereducação, Cibersegurança, Cibercrime, Ataques Informáticos, Segurança da Informação e Prevenção.

3 De acordo com o *Gartner Press Release* (2016), disponível em: http://www.gartner.com/newsroom/id/3165317. [17-04-2017].

ABSTRACT

The internet invention was one of the greatest technological discoveries of humankind and had led to a profound transformation in habits and lifestyles around the world. This allowed access to the information in a matter of seconds. For instance, in 2016 were connected through the Internet 6.4 billion electronic equipment worldwide[4].

However, if the massive use of the Internet offers possibilities of freedom and democracy never before experienced, also it fosters the development of illicit forms of cyberspace.

In fact, cybercrime is a phenomenon that is increasing worldwide, where its impact goes far beyond the traditional economic damages. Actually, cyber-attacks threaten privacy and citizens' freedom, jeopardize the sovereignty of the State and may disclose information that might threaten the national security.

Therefore, in order to build the essential foundations for the effective fight against cybercrime, it is crucial to have a good understanding of this criminal phenomenon, which affects everything and everyone. For that reason, cyber-education is the key to success, and it is essential to collaborate in awareness-raising and political action on cybersecurity.

In summary, this paper discusses the challenges that cyberspace currently poses to all sectors of our society, mainly due to the widespread increase of Cybercrime around the world. In this context, we consider that, the best prevention strategy base on the development of a culture of information security in cyberspace, which would only achieved by implementation of an education policy in our society

Keywords: Cyber-education, Cybersecurity, Cybercrime, Cybercrime, Computer Attacks, Information Security and Prevention.

4 According to Gartner Press Release (2016), available in: http://www.gartner.com/newsroom/id/3165317 [17-04-2017].

ÍNDICE

1. INTRODUÇÃO

Ao longo da última metade do século XX, assistiu-se a uma rápida evolução tenológica, permitindo que as sociedades gerassem elevados índices de crescimento económico e social, e desencadeando o desenvolvimento e adoção de novas Tecnologias de Informação e Comunicação (TIC), as quais moldaram a forma como as pessoas vivem e comunicam entre si, sendo atualmente, vitais ao funcionamento das sociedades modernas.

Neste âmbito, a invenção da Internet[5] como uma rede mundial de computadores, desempenhou um papel fundamental na transformação da sociedade, tendo como consequência última, a criação de um novo espaço que não tem existência física, mas apenas virtual, o qual se denomina de ciberespaço (Schmitt, 2013).

O termo ciberespaço foi utilizado pela primeira vez pelo escritor de ficção científica William Gibson em 1982[6], para descrever um espaço virtual sustentado na interligação de computadores e pessoas à escala global. Com efeito, mesmo considerando a distância temporal que separa a atualidade, da capacidade visionária de Gibson em 1982, verifica-se que o ciberespaço intensificou transformações sociais nos diversos campos da atividade humana, tendo Castells (2002) apelidado de sociedade em rede. Efetivamente, esta nova sociedade, também por diversas vezes denominada por sociedade de

5 A Origem da internet remonta ao período da presidência de Eisenhower nos Estados Unidos da América (EUA), durante a Guerra Fria. Decorrente do lançamento pelos soviéticos do satélite espacial Sputnik, o presidente criou a agência ARPA (*Advanced Research Projects Agency),* em 1957, com o objetivo de juntar um conjunto de cientistas de renome e competência comprovada, para incrementar a tecnologia espacial. A amplitude de matérias coberta pela ARPA levou à criação de vários departamentos especializados. Na área da informática nasceu o IPTO (*Information Processing Techniques Office*). Neste âmbito, um conjunto coincidente de descobertas, desencadeou as fundações da futura internet (Belfiore, 2010).

6 A palavra Ciberespaço foi utilizada pela sua primeira vez pelo escritor de ficção científica William Gibson em 1982, num conto denominado "*Burning Chrome*", publicado na revista *Omni*, para descrever um espaço virtual sustentado na interligação em rede de máquinas e pessoas à escala global, como um "*mass consensual hallucination of computer networks*". O termo viria a ser popularizado mais tarde após a publicação do seu famoso livro "*Neuromancer*" publicado em 1984. Cf. *The Guardian* (2014), disponível em: < https://www.theguardian.com/books/2014/jul/28/william-gibson-neuromancer-cyberpunk-books> [11-01-2017].

informação[7], tem vindo a oferecer um leque alargado de potencialidades para os estados e para os cidadãos.

Porém, a utilização massiva da internet, se por um lado, oferece possibilidades de liberdade e democracia nunca antes vivenciados, por outro, potencia o desenvolvimento de formas ilícitas de utilização do ciberespaço. É neste contexto, que Venâncio (2011) refere que "as especificidades da criminalidade informática colocam-se, não só na transferência de comportamentos ilícitos para o ambiente digital, como na tipificação de novos crimes com elementos caracterizadores de natureza digital".

Neste âmbito, verifica-se que se multiplicam as burlas informáticas e as fraudes financeiras à escala internacional. O cibercrime é um "fenómeno em galopante crescimento" (Ribeiro, 2016). Estima-se que em 2015, à escala global, 549 milhões de pessoas foram vítimas de crime *online*. Esta tendência verificou-se também entre nós. De acordo com o Relatório Anual da Segurança Interna (RASI (2016))[8], o crime de sabotagem informática subiu 140%, o dano relativo a dados ou programas informáticos 121% e a falsidade informática 58%. Acresce que, segundo dados da Direção-Geral de Política de Justiça, também citados no relatório, revelam um aumento dos crimes informáticos de 299 casos em 2006 para 801 em 2016, mais 142 do que no ano anterior (21,5%).

De igual modo, destaca-se ainda que o impacto do cibercrime se traduz na maioria das vezes, na ordem dos milhões de dólares, na destruição de empresas e de reputações (como são os casos do roubo de identidade), provocando um clima de desconfiança e incerteza generalizada, abalando a confiança das organizações. De acordo com o *Special Eurobarometer 423 – Cyber Security Report*[9], as perdas devido a cibercrimes representam

7 Um dos primeiros autores a referir o conceito de Sociedade da Informação foi o economista Fritz Machlup, no seu livro publicado em 1962, *The Production and Distribution of Knowledge in the United States*. Contudo, o desenvolvimento do conceito deve-se a Peter Drucker que, em 1966, no seu livro *The Age of Discontinuity*, refere pela primeira vez uma sociedade pós industrial, em que o poder da economia assenta num novo bem precioso: a informação.

8 Vd. in Relatório Anual de Segurança Interna de 2016, disponível em : https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheActividadeParlamentar.aspx?BID=104739&ACT_TP=RSI [05-04-2017].

9 Relatório elaborado por TNS Opinion & Social, a pedido da *European Commission, Directorate-General Home Affairs*, composto pelos resultados de uma pesquisa feita aos 28 países que constituem a UE, entre

biliões de euros por ano, e estima-se que existem mais de 150.000 vírus e outros tipos de *malware* em circulação. Os resultados apresentados no relatório indicam ainda, que 28% dos utilizadores da Internet na União Europeia (UE) não se sentem confiantes para utilizar os serviços de *homebanking* ou para efetuar compras através da internet.

Neste âmbito, as empresas e, em especial, o sector bancário e os seus clientes estão especialmente expostos ao cibercrime. A prevenção é aqui o elemento chave, dado que, este tipo de criminalidade, está também, relacionada com o facto de as rotinas e os hábitos de vida quotidianos indicarem uma generalizada ausência de sensibilidade para a sua perigosidade. No plano das pessoas predomina a ideia que se encontram imunes a estes tipos de crime, transparecendo até uma clara falta de sentido de responsabilidade para a importância dos procedimentos de cibersegurança, em particular no que respeita à proteção dos códigos de acesso/*password* ou na implementação de rotinas de controlo efetivo dos movimentos no extrato/saldo bancário (Ribeiro, 2016).

No quadro geral das empresas, constata-se a existência de uma falta de investimento em segurança, uma ausência de consciencialização para questões de segurança informática, assim como uma carência na formação dos colaboradores, ou ainda uma incorreta análise de risco.

Neste sentido, por forma fundarem-se as bases essenciais para o combate eficaz ao cibercrime é absolutamente fulcral existir uma boa compreensão deste fenómeno criminoso que afeta tudo e todos, o qual em muitos casos é perpetrado por organizações criminosas altamente organizadas e que operam à escala internacional. Por conseguinte, a cibereducação é a chave para o sucesso, sendo essencial colaborar-se para a consciencialização e ação política no que respeita à cibersegurança.

O presente artigo encontra-se dividido em cinco secções. Na primeira secção é realizado um enquadramento do tema. Na secção seguinte, são descritos os conceitos de Cibersegurança e de Segurança da Informação, os quais são importantes para a compreensão do tema em discussão. Na terceira secção, é abordado de forma sucinta o conceito de cibercrime, e são descritos os principais tipos de ataques informáticos

11 e 20 de outubro de 2014. Disponível em: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_423_en.pdf [05-04-2017].

existentes. O tema da cibereducação é apresentado na quarta secção, apresentando-se um compêndio das principais ofertas formativas na área da cibersegurança existente nas principais Universidades e Institutos Superiores de referência Nacionais nestas matérias. Finalmente, as conclusões são apresentadas na secção cinco.

2. CIBERSEGURANÇA

"Paradoxalmente, a conectividade é o maior problema da segurança. Nações internet-dependentes têm muito mais a perder quando a rede deixar de funcionar. Se os computadores estivessem isolados os problemas de segurança eram muito reduzidos, mas em contraposição, os benefícios da rede, de estar ligado, da conectividade, são demasiados elevados para serem ignorados" (Freire, 2013)

2.1.Enquadramento e Conceito

A invenção da internet foi uma das maiores descobertas tecnológicas da Humanidade, tendo provocado uma transformação profunda nos hábitos e estilos de vida em todo o mundo. Esta permitiu ter acesso à informação numa questão de segundos, podendo referir-se a título de exemplo, que em 2016 estiveram conectados através da internet 6,4 biliões de equipamentos eletrónicos em todo o mundo.

Porém, a utilização massiva da internet, se por um lado, oferece possibilidades de liberdade e democracia nunca antes vivenciados, por outro, potencia o desenvolvimento de formas ilícitas de utilização do ciberespaço. Na realidade, qualquer computador que se ligue à internet, poderá estar em risco porque poderá abrir uma porta para utilizadores mal-intencionados. Por isso, todos os utilizadores dos sistemas de informação necessitam de defender a sua informação dos possíveis atacantes. Neste âmbito, cabe aos Estados, às organizações e a cada um dos utilizadores em particular, exercer o seu papel naquilo que hoje se denomina a cibersegurança. De um modo geral, segundo a ITU (*International Telecommunication Union*), por Cibersegurança entende-se como o "conjunto de ferramentas, de políticas, de conceitos, de orientações, de processos de gestão de risco,

de ações, de atividades de treino e prática que, juntamente com as tecnologias, podem ser utilizados para proteger o ciberespaço bem como a organização e os seus meios"[10].

No essencial, e corroborando com Freire (2013), as questões/soluções de cibersegurança devem ter o seu ponto de partida no valor da informação, mais do que nos aspetos tecnológicos, os quais, embora sejam igualmente importantes e de tratamento obrigatório, são subsequentes. Assim, torna-se fundamental expor-se em seguida, em que consiste e qual a finalidade da Segurança da Informação.

2.2.Segurança da Informação

Segundo a Associação para a Promoção e Desenvolvimento da Sociedade de Informação (APDSI), entende-se a Segurança da Informação como sendo a:

> "*Proteção dos sistemas de informação contra o acesso ou a modificação não autorizados da informação, durante o seu armazenamento, processamento ou transmissão, e contra a negação de serviço a utilizadores autorizados ou o fornecimento de serviço a utilizadores não autorizados, incluindo as medidas necessárias para detetar, documentar e contrariar tais ameaças*" (CNCS, 2017).

Da mesma maneira, e de uma forma simplista poder-se-á referir que a finalidade da Segurança da Informação consiste em garantir que a informação, um dos maiores bens ou ativos das Pessoas, das Organizações e dos Estados, não seja modificada, pervertida, copiada ou eliminada, ou melhor que as suas propriedades[11] se mantenham inalteráveis, designadamente: a confidencialidade, a integridade e a disponibilidade.

---

10 Segundo o Departamento de Segurança Interna dos EUA, Cibersegurança corresponde à Estratégia, política e normas com vista à segurança das operações no ciberespaço, abrangendo missões de redução da ameaça, de vulnerabilidades, de compromisso internacional, de resposta a incidentes, resiliência, e políticas de recuperação, incluído operações em rede, garantia da informação, ações judiciais, diplomáticas, militares e de inteligência relacionadas com a segurança e estabilidade da infraestrutura global de informação e Comunicações (NICCSN, 2015). Disponível em: https://niccs.us-cert.gov/glossary#C [14-01-2017].

11 De um modo geral são reconhecidas estas três propriedades da Segurança da Informação. No entanto, outros autores, ainda que não consensualmente aceites, referem que além da Confidencialidade, Disponibilidade e Integridade, são propriedades da Segurança da Informação, o Não Repúdio e Autenticação (Freire, 2013). Segundo a APDSI (2017) o Não Repúdio é a propriedade que visa garantir que uma mensagem não seja repudiada pelo destinatário, assegurando-lhe que esta se mantém íntegra; por outras palavras, o destinatário deve poder assegurar-se de que a mensagem foi realmente originada pelo

A confidencialidade da informação visa garantir que apenas os utilizadores autorizados podem ter acesso à informação (Kim, 2013). Com efeito, a conectividade numa rede global tem facilitado aos *hackers*[12] o roubo de enormes quantidades de informação, mesmo a mais sensível. Por sua vez, a integridade consiste em salvaguarda o carácter exato e completo da informação (Kim, 2013). Neste âmbito, verifica-se que muitos ataques informáticos se concretizam através da sabotagem de dados, nomeadamente para propósitos criminosos[13], políticos[14] ou militares[15]. Por seu turno, a disponibilidade da informação fundamenta-se na propriedade de estar acessível para consulta ou utilização, por parte de uma entidade autorizada sempre que necessário (Kim, 2013). Por conseguinte, um ataque à disponibilidade dos computadores ou recursos da informação traduz-se na privação dos utilizadores autorizados acederem aos sistemas para o desempenho das suas tarefas.

Por conseguinte, e tal como se infere a partir da Figura 1, a Segurança da Informação envolve uma abordagem sistémica, assente em três pilares fundamentais: Pessoas, Processos e Tecnologias.

alegado remetente, não tendo sido forjada nem alterada na transmissão. Já a autenticidade, segundo a mesma fonte, num contexto informacional, é a propriedade de uma informação cuja origem e integridade são garantidas.

12 Pessoas com grandes conhecimentos de informática e programação, que se dedicam a encontrar falhas em sistemas e redes computacionais "*hacker*", in Dicionário Priberam da Língua Portuguesa [em linha], 2008-2013, https://www.priberam.pt/dlpo/hacker [consultado em 25-01-2017].

13 Exemplo claro deste ataque é o *Ransomware*, o qual segundo o CNCS (2017) representa um tipo de malware (vírus, *trojans*, etc.), que visa bloquear o acesso ao sistema do computador de um dado utilizador. Para que esta restrição seja removida, um *hacker* solicita que seja pago um resgate. O vírus *Wanna Cry* foi o último grande ataque deste tipo, o qual foi despontado no dia 12 de maio de 2017, tendo sido bastante publicitado uma vez que atingiu mais de 125 mil sistemas de computadores, afetando mais de 100 países ((RTP, 2017).

14 Países com menor atenção aos direitos humanos editam e-mails e inibem os blogs dos seus cidadãos (Freire, 2013).

15 Exemplo claro foi o caso do ciberataque que abalou a Estónia em abril de 2007. Concretamente, e alegadamente na sequência da mudança de localização de uma estátua soviética, do centro do Talin para os arredores da cidade, foi vítima de um ataque maciço de negação de serviço (*Distributed Denial of Service* (DDoS)) aos servidores do Estado e de várias empresas, afetando principalmente as comunicações eletrónicas mais importantes do país. Esses ataques, que as autoridades da estónia atribuíram ao governo russo, duraram cerca de 22 dias, tendo provocado uma paralisia económica de consequências bastante gravosas, sendo a primeira vez que um ataque cibernético ameaçou a segurança de um Estado (Nunes, 2013).

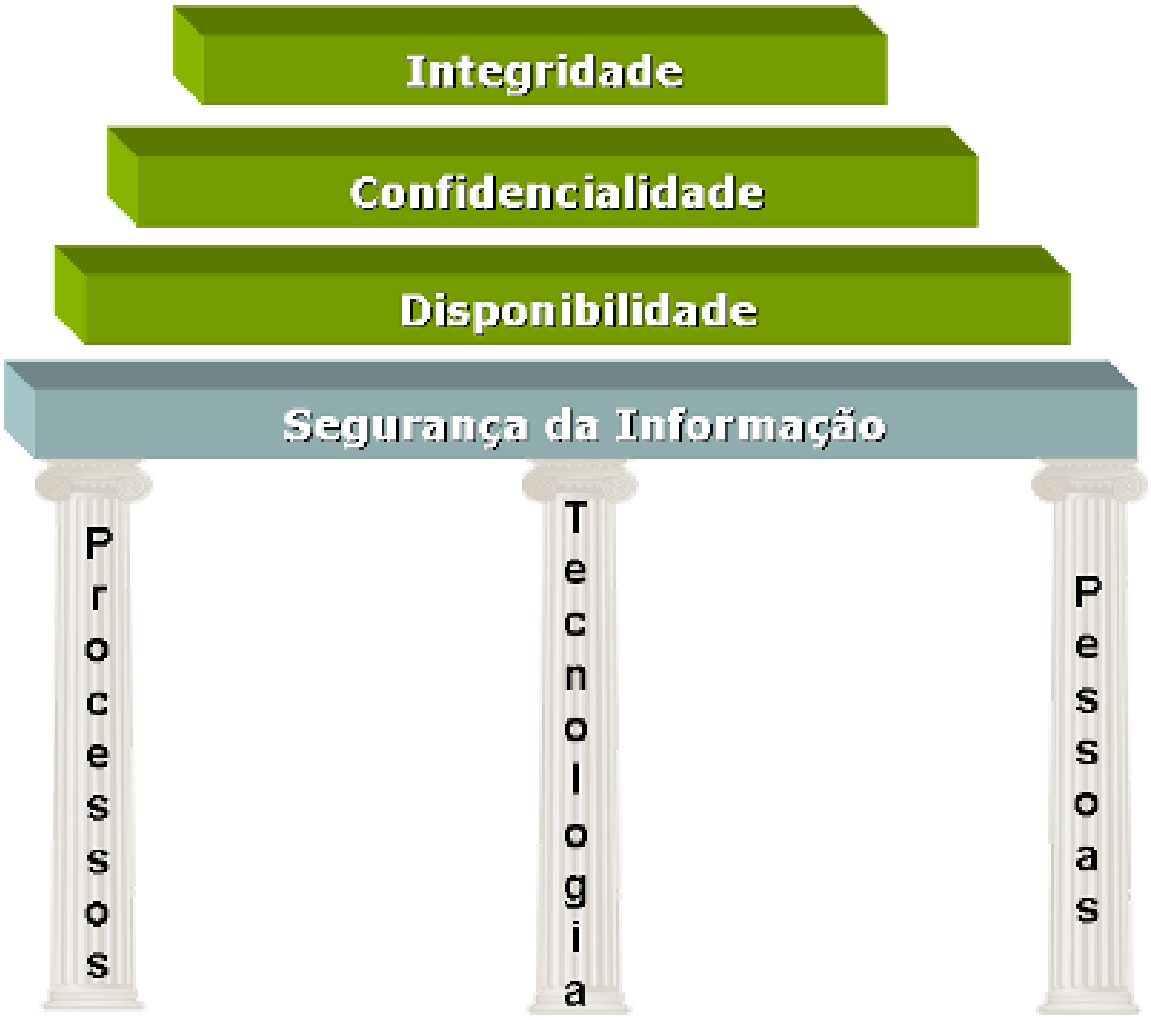


Figura 1 – Pilares da Segurança da Informação (Bernardi, 2011)

Neste sentido, visando garantir-se a segurança da informação dos estados, das empresas, e dos utilizadores em geral, torna-se fundamental, que todos conheçam os processos, que saibam operar e tirar o melhor partido das tecnologias, e que conheçam exatamente os perigos e as vulnerabilidades existentes. Assim, para que este intento seja alcançado, é necessário implementar e desenvolver na nossa sociedade uma forte cultura de cibereducação.

3. CIBERCRIME

"Differ from terrestrial crimes in four ways: They are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present in it; and they are often not clearly illegal" (McConnell Internacional, 2000)

3.1.Enquadramento e Conceito

Em primeiro lugar, importa referir que em virtude de ser um crime praticado através da internet, existem várias terminologias para designar este tipo de criminalidade, tais como cibercrime, crime informático, *high technology crime*, entre outras. Apesar das disposições legais previstas para a criminalidade informática, não existe um conceito expressamente consagrado na lei e uniformemente sedimentado na doutrina e jurisprudência (Marques, 2011).

Neste contexto, perante tal indefinição poder-se-á considerar o conceito amplo defendido por Venâncio (2011), o qual abrange "toda a panóplia de atividade criminosa que pode ser levada a cabo por meios informáticos, ainda que estes não sejam mais que um instrumento para a sua prática, mas que não integra o seu tipo legal, pelo que o mesmo crime poderá ser praticado por recurso a outros meios", em detrimento de um conceito restrito, correspondente aos crimes em que a informática será apenas parte integradora do tipo legal ou seu objeto de proteção.

Coube inicialmente à Lei nº 109/91, Lei da Criminalidade Informática[16], dispor um catálogo de crimes ligados à informática[17], tendo sido, com a participação e posterior assinatura do Tratado da Convenção de Budapeste por parte de Portugal a 23 de Novembro de 2001, revogada pela Lei nº 109/2009, Lei do Cibercrime (LC)[18], a qual

16 Lei n.º 109/91, de 17/8, disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=151&tabela=lei_velhas&nversao=1&so_miolo=[06-04-2017].

17 Lei da Criminalidade Informática definiu um conjunto de crimes ligados à informática, nomeadamente: a falsidade informática, o dano relativo a dados ou programas informáticos, a sabotagem informática, o acesso ilegítimo, a interceção ilegítima, a reprodução ilegítima de programa protegido.

18 Lei n.º 109/2009 de 15/9, Disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis [06-04-2017].

"*veio introduzir novos meios de investigação e produção de prova específicos para o combate à criminalidade informática*" (Venâncio, 2011). Concretamente, o legislador português entre os artigos 3.º e 8.º da LC define como crimes ligados à informática: a falsidade informática, o dano relativo a programas ou dados informáticos, a sabotagem informática, o acesso legítimo, a interseção ilegítima e a reprodução ilegítima de programa protegido. Além destes crimes, o legislador português já havia considerado no Código Penal os crimes de devassa por meio de informática (artigo 193.º), de violação de correspondência (artigo 194.º) e de burla informática e nas telecomunicações (artigo 221.º).

Considerando, todos os tipos legais apresentados, a execução dos crimes informáticos será executado por três formas: através de manipulação, ou alteração de dados; de espionagem, com o furto de dados informáticos; e a sabotagem, destruindo ou danificando parte ou totalmente os dados armazenados.

Por outro lado, em relação à investigação do cibercrime, segundo Dias (2010), os principais problemas com que se deparam os investigadores são os seguintes:

- A falta de legislação adequada;
- A falta de metodologia no tratamento da especificidade deste crime;
- A interoperatividade dos sistemas;
- A lentidão da cooperação e a falta de partilha de informações (quer entre entidades nacionais quer a nível internacional).

Perante esta problemática, e conforme sublinha Verdelho (2003), "as instâncias internacionais manifestam, cada vez mais, preocupação pelas consequências dos atos ilícitos cometidos nas redes, ou através das redes de computadores". Nesse sentido, a Convenção sobre Cibercrime[19] foi um sinal claro da vontade de mudança existente. Com

19 Concluído e aprovado em Novembro de 2001, o Tratado da Convenção sobre o Cibercrime foi apresentado para assinatura e ratificação aos 47 Estados membros, bem como a outros Estados presentes com o estatuto de observadores, entre os quais Estados Unidos da América, Japão, África do Sul e Canadá, de todos os presentes apenas 27 membros assinaram o tratado, enquanto do lado dos observadores todos assinaram. Foi ainda acrescentado um protocolo adicional ao tratado em Janeiro de 200347 com o intuito de abordar as questões de natureza racista e xenófobas no ciberespaço. Até à data foi assinada por 45 Estados membros e ratificada por 40 dos mesmos, 8 Estados não constituintes do Conselho da Europa também procederam à ratificação, de destacar a não assinatura e ratificação de apenas dois Estados

efeito, resta agora que no presente e no futuro, cada estado, organização ou utilizador particular contribua com a sua parte neste processo, conhecendo as causas e origens do cibercrime, possibilitando que sejam tomadas medidas eficazes para o seu combate.

3.2.Ataques Informáticos

Um estudo referente ao ano de 2013, abrangendo 13.022 adultos, entre os 18 e os 64 anos, de 24 países do Mundo, estimou que existam aproximadamente 378 milhões de vítimas de cibercrime por ano, um milhão por dia e 12 a cada segundo (APAV, 2017). Neste âmbito, salienta-se o facto de que na grande maioria dos casos, estas vítimas encontram-se numa posição de particular fragilidade e desproteção, dado que, o cibercrime pelo seu carácter recente, ainda é pouco valorizado e compreendido pela população em geral, e os seus efeitos subestimados.

De igual modo, também no quadro das empresas, uma pesquisa realizada pela consultora *EY* expos que 86 % das empresas não se encontram preparadas para responderem a ataques informáticos. **Este estudo** teve como base as respostas fornecidas por 1.735 organizações de todo o mundo, e pertencentes a 20 setores empresariais distintos. Acresce que, em comunicado, a consultora indica que **57% dos inquiridos já foi vítima de pelo menos um ataque virtual,** e que **42% não possui um plano de prevenção,** para o caso sofrerem um ciberataque (Rodrigues, 2017). Estas conclusões, são tanto ou mais preocupantes, uma vez que segundo o Relatório de Cibersegurança realizado pela cisco[20], mais de um terço das organizações que sofreram um ataque informático em 2016 tiveram perdas superiores a 20 % de clientes, receitas e oportunidades de negócio.

Em seguida, descrever-se-ão sucintamente os principais ataques informáticos existentes[21], por forma a elucidar-se em que consistem e quais são os seus impactos.

membros, Rússia e São Marinho. Este tratado entrou em vigor a dia 01 de Julho de 2004 após ser ratificado por 5 países, dos quais 3 são Estados membros do Conselho de Europa. Vd. *in*: Council of Europe, disponível em: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 [06-04-2017].

20 Vd. *in*: *2016 Anual Report*, disponível em: http://www.cisco.com/c/en/us/about/annual-reports.html [22-04-2017].

21 Para uma consulta mais exaustiva e completa sobre os tipos de vírus, recomenda-se a consulta da base de dados da AVAST, denominada por *Academia de Ameaças Online*, e disponível para consulta em: https://www.avast.com/pt-br/c-online-threats [05.04.2017].

3.3.Tipos de Ataques

3.3.1. Vírus

Os Vírus são uma classe de *software* malicioso (*malware*[22]), o qual tal como um vírus biológico, "infecta" o sistema operativo e programas, com o intuito de prejudicar o desempenho de um computador, ou destruir informação em arquivo. Para este efeito, os vírus procuram manter-se indetetáveis, por forma a infetar mais arquivos, deixando o computador vulnerável para que um cibercriminoso consiga vasculhar a informação que lhe seja útil (p. ex. passwords, números de cartão de crédito, códigos bancários, entre outros). Por sua vez, os denominados *worms***,** são um subconjunto de vírus, que possuem a capacidade de auto-replicar, i.e. enquanto um vírus infeta um programa e necessita desse programa para se disseminar, um *worm* é um programa completo, que por conseguinte, não necessita de outro programa para se disseminar. Com efeito, o *worm* visa tornar um computador infetado vulnerável a outros ataques e provocar um aumento considerável no tráfego de dados, prejudicando o acesso aos serviços de rede (AVAST, 2017).

3.3.2 *Spywares*

São um tipo de *malware*, conhecidos por programas espiões, os quais são geralmente difíceis de se detetarem, e visam recolher informações sobre os hábitos dos utilizadores, o histórico de navegação ou informações pessoais (como números de cartão de crédito), e fornece-la a terceiros através da internet, sem o utilizador se aperceber (AVAST, 2017).

3.3.3.*Distributed Denial of Service (DDoS)*

Os ataques de Negação de Serviço, ou DDoS, visam derrubar *sites* ou redes inteiras sobrecarregando-as com tráfego proveniente de milhares de computadores infetados, e que fazem parte de redes conhecidas como as *botnets*. Os *sites* de bancos, de notícias e até de governos são os principais alvos de ataques de DDoS (AVAST, 2017).

22 *Malware*, é um s*oftware* ou *firmware* que se destina a executar processos não autorizados que terão um impacto adverso na confidencialidade, integridade, ou disponibilidade num Sistema de Informação. Um vírus, um *worm*, ou outra estrutura de código que infete uma máquina. *Spyware* e algumas formas de *adware* são exemplos de código malicioso (NIST N. I., 2013).

3.3.4. *SQL Injection*

A sigla significa "*Structure Query Language*", isto é, consiste numa linguagem de consulta estruturada, que é utilizada para comunicar com bases de dados. Na prática, uma *injection* visa essencialmente encontrar vulnerabilidades num sistema, permitindo a um atacante o roubo de informação (incluindo *passwords* e dados de cartões de credito), ou ainda, incluir por exemplo, conteúdos não desejados num determinado *site* (AVAST, 2017).

3.3.5.*Defacement*

Tipo de ataque que visa modificar o conteúdo de um *site*, normalmente feito como forma de protesto ou *hacktivismo*[23] (Neves, 2015).

3.3.6.*Cross-site scripting (XSS)*

Este ataque permite a um atacante inserir *scripts* maliciosos em páginas e aplicativos que seriam à partida confiáveis, e utiliza-los como suporte de dados ocultos, que irão instalar *malwares* nos navegadores dos utilizadores. Com XSS, os *hackers* não têm como alvo utilizadores específicos, mas em vez disso, procuram disseminar o *malware* pelo máximo de utilizadores possíveis (AVAST, 2017).

3.3.7.*Phishing*

Este ataque consiste no envio de mensagens de correio eletrónico, aparentemente provenientes de organizações financeiras credíveis, mas com ligações para falsos *sites* que são replicas dos originais, e nos quais, é solicitado ao utilizador a atualização dos seus dados privados. Desta forma, os atacantes irão conseguir que sejam reveladas informações pessoais, como *passwords*, códigos de cartão de crédito, ou número de contas bancárias (CNCS, 2017).

23 Sucintamente, por *Hacktivismo* entende-se como a ação conduzida por indivíduos ou grupos, que utilizam os meios informáticos e "veem a Internet como um veículo para promover e catalisar as suas causas e disseminar a sua mensagem" (Santos, 2011, p. 27).

3.3.8.*Botnets*

Uma *botnet* é uma rede de computadores que foram infetados por *softwares* maliciosos, podendo deste modo ser controlados remotamente, de forma por exemplo, a enviar *spam*[24], a disseminar vírus ou ainda a executar ataques de DDoS, sem o conhecimento ou o consentimento dos proprietários dos computadores infetados (AVAST, 2017).

3.3.9.*Ransomware*

Um ataque r*ansomware* representa um tipo de *malware* (vírus, *trojans*, etc.) que infeta os sistemas informáticos dos utilizadores e manipula o sistema para que uma vítima não consiga utilizar, parcial ou totalmente, o seu computador, e por conseguinte os dados que possui em arquivo. A vítima geralmente recebe um aviso que se encontra a ser vítima deste ataque por *pop-up*, sendo deste modo pressionado a pagar um resgate para recuperar o acesso total ao sistema e aos arquivos.

Posto isto, e passados que estão em revista, os principais tipos de ataques informáticos, conclui-se que os utilizadores comuns da internet apenas poderão evitar e fazer face, à panóplia e complexidade de ataques existentes se souberem os perigos que existem ao utilizar a internet e como os evitar. Para tal é fundamental, fomentar-se uma cultura de cibereducação nos nossos cidadãos.

Neste sentido, irá ser apresentada em seguida um levantamento da oferta formativa em matéria de cibersegurança existente nas principais Universidades e Institutos Superiores de referência nacionais.

24 O *Spam*, são mensagens de correio eletrónico não solicitadas, geralmente enviadas de uma forma massiva e indiscriminada, que, para além do incómodo provocado aos utilizadores do correio eletrónico, podem comprometer o bom funcionamento dos sistemas informáticos (CNCS, 2017).

4. CIBEREDUCAÇÃO – OFERTA FORMATIVA DE UNIVERSIDADES E INSTITUTOS SUPERIORES NACIONAIS

"*O principal objetivo da educação é criar pessoas capazes de fazer coisas novas e não simplesmente repetir o que as outras gerações fizeram"* (Jean Piaget")[25]

No Instituto Superior Técnico (IST), da Universidade de Lisboa, a Segurança da Informação afigura-se como sendo uma área ativa de ensino, de investigação e de cooperação internacional. Verifica-se que existe nesta instituição, uma ligação muito próxima ao Instituto de Telecomunicações (IT) e ao seu Grupo de Segurança e Informação Quântica, e ao Instituto de Engenharia de Sistemas e Computadores (INESC). Simultaneamente, a sua atividade traduz-se neste âmbito, na publicação de dezenas de artigos científicos anualmente, na realização de projetos científicos e no provimento de serviços de consultadoria a empresas e organismos do Estado, incluindo o Gabinete Nacional de Segurança, bem como ainda, na formação avançada de especialistas, materializada pelo programa de Doutoramento em Segurança da Informação do IST.

Existe ainda, nesta instituição duas ofertas curriculares específicas nesta matéria, nomeadamente: o Mestrado Integrado de Engenharia Eletrotécnica e de Computadores[26]; e o Mestrado de Segurança da Informação e Direito do Ciberespaço (MSIDC)[27]. No primeiro, destaca-se a cadeira de Segurança Informática em Redes e Sistemas, cujo objetivo, consiste em disponibilizar um conjunto de conceitos, metodologias e ferramentas de segurança informática. Por sua vez, o segundo é uma iniciativa conjunta do IST e da Faculdade de Direito, da Universidade de Lisboa (FDUL), e da Escola Naval (EN), que visa proporcionar uma formação científica especializada nesta área multidisciplinar apoiada na complementaridade das valências das três instituições, reforçando a articulação entre teoria, prática e investigação nestes domínios, e contribuir assim para dotar o país das competências necessárias para enfrentar os desafios que se colocam.

25 Fonte *Wikiquote* 2017, disponível para consulta em: https://pt.wikiquote.org/wiki/Jean_Piaget [18-04-2017].
26 Disponível em: https://fenix.tecnico.ulisboa.pt/cursos/meec [18-04-2017].
27 Disponível em: https://fenix.tecnico.ulisboa.pt/cursos/msidc [18-04-2017].

De igual modo, a Faculdade de Ciências da Universidade de Lisboa (FCUL) proporciona a frequência do Mestrado em Segurança Informática[28], o qual pretende dar formação aos licenciados e profissionais na área da segurança da informação e suas aplicações (ex. ERP, ASP, e-comércio, e-finança), incluindo a segurança e a confiabilidade de infraestruturas críticas (ex. redes elétricas ou redes de telecomunicações).

Por sua vez, no Instituto Superior de Estatística e Gestão de Informação (ISEGI), da Universidade Nova de Lisboa, verifica-se que existe no plano de curso da Licenciatura em Sistemas e Tecnologias de Informação (TIC) a unidade curricular Segurança Informática[29], a qual tem como objetivo compreender, aplicar e gerir a segurança informática em computação, comunicação e sistemas organizacionais. Concretamente, verifica-se que nesta cadeira são abordados aspetos operacionais como políticas e procedimentos, mecanismos de ataque e defesa, análises de risco, entre outos.

Mais a Sul, na região do Alentejo e sub-região do Baixo Alentejo, o Instituto Politécnico de Beja disponibiliza aos seus alunos o Mestrado de Segurança Informática[30], o qual se caracteriza por uma forte componente de ensino prático de segurança ofensiva. Concretamente, nesta instituição ensinam-se técnicas de ataque a sistemas informáticos, com grande componente prática, para formar profissionais com uma consciência "de facto" sobre as medidas de segurança necessárias. Em termos práticos, este mestrado permite a formação de especialistas com as seguintes competências principais: (i) realização de testes de penetração em sistemas informáticos; (ii) pesquisa, seleção, reutilização e desenvolvimento de *exploits* para sistemas informáticos; (iii) realização de perícias forenses a sistemas informáticos; (iv) desenvolvimento de sistemas de informação e de *software* seguro; (v) especificação de equipamentos de identificação biométrica e integrá-los em sistemas de segurança.

28 Disponível em: https://ciencias.ulisboa.pt/pt/evento/18-04-2016/sess%C3%A3o-de-apresenta%C3%A7%C3%A3o-do-mestrado-em-seguran%C3%A7a-inform%C3%A1tica [18-04-2017].
29 Disponível em: http://www.unl.pt/guia/2013/isegi/UNLGI_getUC?uc=82036 [18-04-2017].
30 Disponível em: https://www.flickr.com/photos/40478366@N08/sets/72157669259472641 [18-04-2017].

Já na região centro, a Universidade de Coimbra (UC) vai lecionar a partir do próximo ano letivo (2017/2018), um Mestrado em Segurança Informática (MSI)[31], o qual será ministrado pelo Departamento de Engenharia Informática da Faculdade de Ciências e Tecnologia (FCTUC) em colaboração com a Faculdade de Direito (FDUC). Segundo o coordenador deste mestrado, Eduardo Monteiro, o MSI "terá uma forte ligação às empresas e ao mercado laboral porque as necessidades de competências na área da segurança informática são cada vez mais prementes, existindo uma grande carência de profissionais com competências específicas nesta área" (Monteiro, 2017).

Por sua vez na Beira Litoral, a Universidade de Aveiro (UA), disponibiliza quatro unidades curriculares nesta matéria, designadamente: Segurança[32], Segurança e Gestão de Risco[33], Segurança Informática nas Organizações[34] e Segurança Avançada em Redes[35]. A primeira tem como objetivo geral apresentar e descrever os principais conceitos fundamentais da segurança em sistemas computacionais. Já a Segurança e Gestão de Risco, têm como finalidade dar as bases e as ferramentas para que seja desenvolvida e implementada uma política de segurança na organização, e ainda fornecer as bases para o desenvolvimento e aplicação de um processo de gestão do risco. A terceira unidade curricular tem como objetivo fornecer uma visão geral na temática da Segurança Informática. Por fim, a unidade curricular Segurança Avançada em Redes, expõe e descreve as diversas vulnerabilidades dos sistemas computacionais ligados em rede.

Por seu turno, a Faculdade de Ciências da Universidade do Porto (FCUP) dispõe de um Mestrado em Segurança Informática[36], que proporciona aos seus alunos uma formação avançada na área da cibersegurança. Este curso visa melhorar os conhecimentos técnicos e práticos de segurança informática dos licenciados que pretendam seguir uma carreira profissional nesta área, e simultaneamente, cimentar os conceitos teóricos daqueles que queiram prosseguir uma formação académica.

31 Disponível em: http://www.uc.pt/en/fctuc/dei/COURSES/MSI [27-06-2017].
32 Disponível em: http://www.ua.pt/deti/uc/2834 [19-04-2017].
33 Disponível em: http://www.ua.pt/deti/uc/6489 [19-04-2017].
34 Disponível em: http://www.ua.pt/uc/4143 [19-04-2017].
35 Disponível em: http://www.ua.pt/deti/uc/6248 [19-04-2017].
36 Disponível em: https://sigarra.up.pt/fcup/pt/web_page.inicial [19-04-2017].

Mais a norte ainda, na Universidade do Minho, existe no plano de curso do Mestrado em Engenharia Informática, uma unidade curricular denominada Criptografia e Segurança de Sistemas de Informação[37]. Esta UC tem como alvo a segurança da informação e a confiabilidade dos sistemas informáticos. Pretende-se, entre diversos objetivos, que os formandos conheçam e dominem as diversas vertentes da administração de sistemas informáticos como forma de assegurar segurança e correção e também conheçam, selecionem e apliquem técnicas de desenvolvimento de aplicações seguras.

5. CONCLUSÃO

A sociedade de informação em que vivemos, caraterizada pela total dependência das TIC e pelo seu funcionamento em rede aberta, sem delimitação de fronteiras físicas, acarreta novos desafios de segurança, em virtude das vulnerabilidades inerentes às propriedades do ciberespaço. Como resultado deste facto, constata-se que estas vulnerabilidades têm sido aproveitadas pelos cibercriminosos, os quais se têm dedicado ao longos dos últimos anos a criar, desenvolver e implementar uma panóplia de ataques informáticos, que tem afetado gravemente os Estados, as empresas e os cidadãos de todo o mundo. Com efeito, conforme sublinhou Ribeiro (2016), o cibercrime é um "fenómeno em galopante crescimento", com consequências e impactos transversais a toda a sociedade.

Neste sentido, para que seja alcançada, garantida e fomentada a cibersegurança na nossa sociedade, é fundamental apostar-se na prevenção, a qual se afigura ser a melhor forma de detetar, evitar e combater os efeitos do cibercrime. Neste âmbito, considera-se que a prevenção somente será alcançada com a aposta em dois pilares fundamentais, nomeadamente: o desenvolvimento tecnológico e a formação dos utilizadores.

Em relação ao desenvolvimento tecnológico, considera-se ser fundamental aos Estados e às Organizações efetuarem um investimento tecnológico e financeiro que permita, por um lado, a implementação de medidas de proteção eficazes, e por outro, o

37 Disponível em: http://mei.di.uminho.pt/?q=pt-pt/1213/cssi [19-04-2017].

desenvolvimento de infraestruturas de segurança que possibilitem antever o surgimento de novas formas de cibercrime.

Quanto à formação, considera-se efetivamente que, para que sejam criadas as bases para o combate eficaz ao cibercrime, é fulcral existir uma boa compreensão deste fenómeno criminoso que atinge tudo e todos, e que em muitos casos é perpetrado por organizações criminosas altamente organizadas e que operam à escala internacional. De facto, o conhecimento das causas e origens do cibercrime permitirá, que sejam tomadas medidas mais concretas e eficientes para o seu combate. Neste sentido, para que este desígnio de prevenção seja alcançado, é fundamental desenvolver e implementar uma política de cibereducação na nossa sociedade. Com efeito, e embora existam no ciberespaço, soluções tecnológicas que permitem mitigar muitos dos problemas vigentes, na prática, conforme menciona Pedro Veiga (2016), caso os gestores não estejam conscientes dos problemas existentes, não as aplicarão nas organizações e nas empresas que administram, ou não atribuirão os recursos humanos e meios materiais necessários para garantir a cibersegurança organizacional.

Por outro lado, no que concerne ao levantamento realizado ao nível da formação de cibersegurança existente nas principais Universidades e Institutos Superiores de referência nacionais, constata-se que esta é ainda escassa. No entanto, denota-se que certas instituições começam já, por desenvolver um esforço para proporcionarem cursos que permitam um conhecimento mais profundo na área da cibersegurança.

Não obstante, considera-se que a base para se efetuar uma partilha de informação com segurança deve ter origem nas matérias lecionadas durante o percurso académico de qualquer utilizador, adaptadas aos diferentes níveis de ensino.

Com efeito, logo no ensino básico e secundário, onde os adolescentes são grandes consumidores de novas tecnologias, deveria ser ministrada formação sobre as vulnerabilidades dos sistemas que utilizam, e quais as medidas de prevenção que podem implementar para se protegerem.

Por seu turno, no ensino superior, matérias no âmbito da Segurança da Informação e a da Segurança Informática deveriam fazer parte de todos os cursos do ensino superior, independentemente, de os alunos pertencerem a áreas tecnológicas ou das ciências sociais. Com efeito, um utilizador comum, em alguma fase da sua atividade profissional irá utilizar um Sistema de Informação e Comunicação (SIC) e ser responsável pela gestão da informação, sendo por conseguinte, essencial conhecer as vulnerabilidades existentes, e quais as medidas de proteção que estão à sua disposição para evitar sofrer um ataque informático.

Em suma, a cibereducação é, efetivamente, uma competência que deve ser lecionada na atividade formativa de cada cidadão e é da responsabilidade do Estado incluir este tema nos programas de formação.

6. BIBLIOGRAFIA

Albaret-Schulz, C. A. (2004). *La frontière, un object spatial en mutation.* Fonte: EspacesTemps.net: http://www.espacestemps.net/document842.html

APAV. (2017). *A realidade do Cibercrime*. Fonte: APAV - Cibercrime: http://www.apav.pt/cibercrime/

APDSI. (2017). *Glossário*. Fonte: APDSI.PT: http://www.apdsi.pt/index.php/portugues/menu-secundario/glossario.html

August, O. (2007). *The Great Firewall: China's Misguided – and Futile – Attempt to Control What Happens Online.* Acesso em 05 de 01 de 2017, disponível em Wired Magazine: http://archive.wired.com/politics/security/magazine/15-11/ff_chinafirewall?currentPage=all

AVAST. (2017). *Academia de Ameaças Online*. Fonte: AVAST: https://www.avast.com/pt-br/c-online-threats

Belfiore, M. (2010). *The Department of Mad Scientists.* Nova Iorque: Harper Perennial.

Bernardi, F. (2011). Segurança da Informação - Consciencialização. Rio de Janeiro. Fonte: http://www.bluminformatica.com.br/SegurancadaInformacaoConscientizacao.html

Cabreiro, C. (2016). Cibercrime. *Curso Geral de Cibersegurança: Uma perspetiva Whole-of-Society*. Lisboa.

Caetano, M. (1973). *Manual de Ciência Política e Direito Constitucional.* Coimbra: Coimbra Editora.

Carvalho, J. S. (2009). Segurança Nacional, Serviços de Informações e as Forças Armadas. *Segurança e Defesa n.º 11*.

Castells, M. (2002). *A Era da Informação: Economia, Sociedade e Cultura, Vol. I - A Sociedade em Rede.* Lisboa: Fundação Calouste Gulbenkian.

Castells, M. (2009). *Communication Power.* Oxford: Oxford University Press.

CEDN. (2013). Resolução do Conselho de Ministros N.º 26/2013 (D.R. N.º 77, 1.ª Série). Lisboa: Diário da República.

Churchill, W. S. (1968). *World Crisis.* Potterne, United Kingdom: M Godding Books Ltd.

Clark, D. (2010). *Characterizing cyberspace: past, present and future.* MIT. Acesso em 09 de 01 de 2017, disponível em https://projects.csail.mit.edu/ecir/wiki/images/7/77/Clark_Characterizing_cyberspace_1-2r.pdf

CNCS. (2017). *Glossário*. Fonte: Centro Nacional de Cibersegurança Portugal: https://www.cncs.gov.pt/recursos/glossario/

CNN. (2016). *2008 Georgia Russia Conflict Fast Facts*. Fonte: CNN Library: http://edition.cnn.com/2014/03/13/world/europe/2008-georgia-russia-conflict/

Demchak, C. & Dombrowski, P. (2011). Rise of Cybered Westephalian Age. *Strategic Studies Quarterly*, 32-61. Acesso em 13 de 01 de 2017, disponível em http://www.au.af.mil/au/ssq/2011/spring/demchak-dombrowski.pdf

Denning, D. E. (2010). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. *J. Arquilla and D. F. Ronfeldt (eds)*, 239-288.

Dias, V. (2010). *A Problemática da Investigação do Cibercrime - I Curso Pós Graduação de aperfeiçoamento em Direito da Investigação criminal e da prova.* Lisboa: Universidade de Lisboa – Faculdade de Direito. Fonte: http://www.verbojuridico.com/doutrina/2011/veradias_investigacaocibercrime.pdf>

ENISA. (2011). *Protecting Industrial Control Systems - Recommendations for Europe and Member States.* Brussels: ENISA. Acesso em 27 de 12 de 2016, disponível em https://www.enisa.europa.eu/publications/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states

Fernandes, A. J. (1995). *Introdução à Ciência Política.* Porto: Porto Editora.

Fernandes, J. (2012). Utopia, Liberdade e Soberania no Ciberespaço. Em IDN, *Cibersegurança* (pp. 11-31). Lisboa: IDN.

Freire, V. C. (2013). *Cibersegurança: das preocupações à Ação.* Lisboa: IDN.

GEERS, K. (2008). Cyberspace and the changing nature of warfare. *SC Magazine*, 3-5.

Gobierno de España. (2011). *Estrategia Española de Seguridad: Una responsabilidad de todos.*

Goldsmith J. & Wu, T. (2006). *Who Controls the Internet?: Illusions of a Borderless World* . Oxford University Press, .

Heads of State and Government. (2010). Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation. Lisboa.

IDN. (2013). *Estratégia da Informação e Segurança no Ciberespaço: Investigação conjunta IDN-CESEDEN.* Lisboa: Instituto da Defesa Nacional.

IDN. (2013). *A Defesa Nacional no Contexto da Reforma das Funções de Soberania do Estado.* Lisboa: IDN. Acesso em 14 de 01 de 2017, disponível em http://www.idn.gov.pt/index.php?mod=008&cod=13032013x2#sthash.Ni6K6Xak.dpbs

ITU-T. (2008). *Recommendation ITU-T X.1205 - Overview of Cybersecurity.* ITU.

Jornal I. (2013). E*stónia. Aqui as árvores têm superpoderes*. Fonte: Ionline: https://ionline.sapo.pt/356414

Kim, D. M. (2013). *Fundamentals of Information Systems Security.* Burlington: Jones & Bartlett Learning.

Leite, A. (2016). A Problemática da Cibersegurança e os seus Desafios. doi:http://cedis.fd.unl.pt/a-problematica-da-ciberseguranca-e-os-seus-desafios/

Lourenço, N. (2015). As novas fronteiras da Segurança -Segurança Nacional. Globalização e Modernidade. *Segurança e Defesa*, 26-36.

Marchueta, M. (2002). *O Conceito de Fronteira na Época da Mundialização.* Lisboa: Cosmos.

Martins, M. (2012). Ciberespaço: Uma nova realidade para a Segurança Nacional. Em IDN, *Cibersegurança* (pp. 32-47). Lisboa: IDN.

McConnell Internacional. (December de 2000). Cyber crime…and Punishment? Archaic laws Threaten Global Information.

Mello, C. A. (1999). A Soberania através da História. *Anuário Direito e Globalização: a soberania*.

Miranda, J. (2003). *Manual de Direito Constitucional, Tomo I.* Coimbra: Coimbra Editora.

Miranda, J. (2011). *Manual de Direito Constitucional - Actividade Constitucional do Estado* (4ª Edição ed., Vol. Tomo V). Coimbra Editora.

Moreira, A. (1997). *Teoria das Relações Internacionais* (2ª ed. ed.). Coimbra: Aldemina.

Moreira, A. (2011). *A Circunstância do Estado Exíguo* (3ª Ed. ed.). Loures: Diário de Bordo.

Natário, R. (2013). O Combate ao Cibercrime: Anarquia e Ordem no Ciberespaço. *Revista Militar, 2541*.

Neves, B. (2015). *CAPACIDADE DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO NO CIBERESPAÇO UMA ABORDAGEM DOTMLPI-I.* Lisboa: Instituto Superior Técnico. Acesso em 05 de 01 de 2017, disponível em https://fenix.tecnico.ulisboa.pt/cursos/msidc/dissertacoes

Nunes & Natário. (2014). Risco Social no Ciberespaço. A Vulnerabilidade das Infraestruturas Críticas. *Revista Militar*, 249-286. Acesso em 28 de 12 de 2016, disponível em https://www.revistamilitar.pt/artigo/913

Nunes, P. V. (2004). Ciberterrorismo: Aspectos de Seguranças. *Revista MIlitar*, 1-19. Acesso em 13 de 01 de 2017, disponível em https://www.revistamilitar.pt/artigopdf/428

Nunes, P. V. (2012). *A Definição de uma Estratégia Nacional de Cibersegurança.* Cibersegurança, N.º133, IDN.

Nunes, V. (2013). A Definição de uma Estratégia Nacional de Cibersegurança. Em IDN, *Cibersegurança* (pp. 113-127). Lisboa: IDN.

OTAN. (2014). *Wales Summit Declaration.* Fonte: North Atlantic Treaty Organization: http://www.nato.int/cps/en/natohq/official_texts_112964.htm

Pereira, A. C. (2003). A Soberania no Estado Contemporâneo. *Carta Mensal, 48*.

Pereira, J. (2012). Cibersegurança – O Papel do Sistema de Informações da República Portuguesa. (S. e. Defesa, Ed.) *Segurança e Defesa*.

Republic of Austria. (2013). *Austrian Cyber Security Strategy.* Viena, Áustria: Federal Chancellery.

Resolução do Conselho de Ministros nº 36/2015. (2015). Resolução do Conselho de Ministros nº 36/2015. *Estratégia Nacional de Segurança do Ciberespaço, Diário da República I Série, 113, 12 de junho de 2015*.

Ribeiro. (2016). Cibercrime e "ciberignorância". Lisboa. Acesso em 22 de 03 de 2017, disponível em https://www.publico.pt/2016/06/10/economia/noticia/cibercrime-e-ciberignorancia-1734680

Ribeiro, A. (2001). A retórica dos limites. Notas sobre o conceito de fronteira. Em B. Santos, *Globalização: fatalidade ou utopia?* (pp. 463-488). Porto: Afrontamento.

Rodrigues, M. P. (2017). *Ataques informáticos. As empresas portuguesas estão preparadas?* Fonte: Observador: http://observador.pt/2017/03/26/ataques-informaticos-empresas/

RTP. (2017). *O que deve fazer perante o vírus informático Wanna Cry*. Fonte: RTP: https://www.rtp.pt/noticias/tecnologia/o-que-deve-fazer-perante-o-virus-informatico-wanna-cry_n1001735

Santos, A. R. (2005). *As Metamorfoses do Estado - Rumo à Mega-Confederação Europeia?* Coimbra: Almedina.

Santos, J. L. (2011). *Contributos para uma melhor governação da cibersegurança em Portugal.* Lisboa.

Santos, L. (2001). *Segurança e Defesa na Viragem do Milénio.* Mira: Publicações Europa-America.

Santos, P., e Bessa R. (2008). *Cyberwar - O Fenómeno, as Tecnologias e os Atores.*

Schmitt, M. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare* . Universidade de Cambridge.

Schmitt, M. N. (2013). *Tallin Manual on the International Law Applicable to Cyber Warfare.* UK: Cambridge University Press.

Shea, D. A. (2003). *Critical Infrastructure: Control Systems and the Terrorist Threat.* The Library of Congress. Acesso em 2016 de 12 de 26, disponível em https://fas.org/irp/crs/RL31534.pdf

Sousa, M. R. (1978). *Direito Constitucional, I - Introdução à Teoria da Constituição.* Braga: Livraria Cruz.

TCOR Ralo, J. (2013). *CiberSegurança e CiberDefesa.* Artigo de Opinião.

Techopedia. (2017). *Definition - What does defacement mean*. Fonte: Techopedia: https://www.techopedia.com/definition/4870/defacement

The Guardian. (2014). *William Gibson: the man who saw tomorrow* . Fonte: The Guardian: https://www.theguardian.com/books/2014/jul/28/william-gibson-neuromancer-cyberpunk-books

Traynor, I. (2007). Russia accused of unleashing cyberwar to disable Estonia. *The Guardian*. Brussels. Fonte: https://www.theguardian.com/world/2007/may/17/topstories3.russia

USArmy. (2010). *TRADOC Pamphlet 525-7-8 Cyberspace Operations Concept Capability Plan.* The United States Army.

Veiga, P. (JUNHO de 2016). ENTREVISTA COM O COORDENADOR DO CENTRO NACIONAL DE CIBERSEGURANÇA PORTUGUÊS. *CYBERLAW*, pp. 7-16.

Venâncio, P. (2011). *Lei do Cibercrime.* Lisboa: Coimbra Editora.

Verdelho, P. (2003). Direito da Informação. *Coimbra Editora*, 347-383.

Viana, V. (2012). Prefácio. Em IDN, *Cibersegurança* (pp. 5-7). Lisboa: IDN NAÇÃO E DEFESA.

Vieira, S. (2016). *Segurança da Informação no Ciberespaço – A Cibereducação no caminho da Cibersegurança.* Lisboa: Escola Naval.

White House. (2011). *International Strategy For Cyberspace: Prosperity, Security, and Openness in a Networked World.* White House.

Wolton, D. (1999). *E depois da Internet?* Algés: Difel.

CYBERBULLYING: EDUCAR PARA PROTEGER

CYBERBULLYING: EDUCATE TO PROTECT

ARMANDA PINTO DA MOTA MATOS [1]

1 Faculdade de Psicologia e de Ciências da Educação da Universidade de Coimbra. Correio eletrónico: armanda@fpce.uc.pt.

RESUMO

O rápido desenvolvimento tecnológico ocorrido ao longo dos últimos anos alterou incomensuravelmente o modo, os tempos e os contextos de comunicação entre as pessoas. Os diferentes meios de comunicação, suportados pelas tecnologias digitais, convergem crescentemente para plataformas únicas, que oferecem aos seus utilizadores inúmeras possibilidades para a difusão de informação e para a interação social.

Os *media* digitais constituem para as crianças e os jovens contextos privilegiados para a comunicação e a interação com os pares, assumindo para os mesmos um importante significado social. No entanto, as possibilidades de comunicação oferecidas por estes *media* trazem consigo, a par de inúmeros benefícios, alguns riscos que têm vindo a preocupar a sociedade em geral, pais e todos aqueles que têm responsabilidades educativas. Entre esses riscos, o *cyberbullying* tem recebido crescente atenção, associada ao impacto que esta forma de agressão pode ter em todos os envolvidos.

Este artigo apresenta uma reflexão sobre a problemática do *cyberbullying*, enquadrando-a num contexto comunicacional caracterizado pelo crescente protagonismo dos dispositivos móveis que, ao colocarem no bolso das crianças e dos jovens inúmeras possibilidades de acesso à informação, de entretenimento e em especial de comunicação e interação social, desafiam os modelos e as práticas tradicionais de supervisão e de mediação.

Palavras-chave: *media* digitais, crianças e jovens, ciberespaço, *cyberbullying*, educação.

ABSTRACT

The rapid technological development over the last few years has immeasurably altered the forms, the times and the contexts of communication between people. The different media, supported by digital technologies, increasingly converge to single platforms, which offer its users numerous possibilities for the diffusion of information and social interaction.

In the particular case of children and young people, digital media constitute privileged contexts for communication and interaction with peers, assuming for them an important social meaning. However, the possibilities of communication offered by these media bring with them, along with numerous benefits, some risks which are a cause of concern among society in general, parents and all those who have educative responsibilities. Among those risks, cyberbullying has been receiving increased attention, which is related to the impact that this form of aggression can have on all involved.

This article presents a reflection on the problem of cyberbullying, framing it in a communication context characterized by the growing role of mobile devices, which place in children's and young people' pockets innumerable possibilities for access to information, entertainment and especially communication and social interaction, and thus challenge the traditional models and practices of supervision and mediation.

Keywords: digital media, children and young people, cyberspace, cyberbullying, education.

1. INTRODUÇÃO

O desenvolvimento das tecnologias da informação e da comunicação (TIC) tem vindo a oferecer aos cidadãos, ao longo dos últimos anos, inúmeras oportunidades de entretenimento, fontes de informação infindáveis e novos contextos e formas de comunicação. Desde sempre mediadores da nossa relação com o mundo, extensões dos nossos sentidos (McLuhan, 1964), na atualidade os *media* oferecem oportunidades novas para ultrapassar as barreiras do tempo e do espaço físico. Neste contexto de constantes inovações, os cidadãos têm vindo, progressivamente, a tornar-se, eles próprios, produtores de mensagens e de textos mediáticos, atualizando o conceito de homem EMEREC, proposto por Cloutier há várias décadas atrás (1975).

No caso das crianças e dos jovens, as novidades em termos de equipamentos, aplicações e outros recursos são particularmente exploradas. Na verdade, as crianças e os jovens têm vindo a eleger os *media* digitais, em particular os *media* sociais, como contexto privilegiado para a comunicação e a interação com os pares, de tal modo que a sua realidade quotidiana flui, em continuidade, entre o espaço *offline* e o espaço *online*. Para essa fluidez contribui largamente a progressiva libertação dos constrangimentos espaciais, que a generalização do uso dos dispositivos móveis veio permitir. Com efeito, os dispositivos móveis têm vindo a assumir um crescente protagonismo, como demonstra o Inquérito à Utilização de Tecnologias da Informação e da Comunicação pelas Famílias (INE, 2016), cujos resultados revelam que 72% dos internautas acedem à Internet em mobilidade, sendo os equipamentos mais utilizados o telemóvel/*smartphone* (78%) e o computador portátil (73%). O crescimento do uso do *smartphone* é igualmente evidenciado pelo estudo *Google Consumer Barometer - The Internet in Numbers 2012 – 2016* [1], no âmbito do qual 23% dos utilizadores da Internet em Portugal declararam usar o *smartphone* mais vezes do que o computador ou o *tablet* para aceder à Internet, sendo esta percentagem mais elevada entre os menores de 25 anos (32%) e decrescendo com a idade. O estudo realizado no âmbito do projeto *Net Children Go Mobile*, com crianças e

1 Disponível em https://www.consumerbarometer.com/en/

adolescentes entre os 9 e os 16 anos, revelou a mesma tendência de uso crescente do *smartphone*, sendo de 35% a percentagem de crianças e adolescentes portugueses que afirmam usar este equipamento para aceder diariamente à Internet (Simões, Ponte, Ferreira, Doretto & Azevedo, 2014). Vivemos no tempo da *Internet de bolso*, que mantém permanentemente conectados os cidadãos, especialmente as crianças e os jovens que interagem nos *media* sociais em casa, no quarto, na rua e na escola.

Entre as várias atividades realizadas *online*, a participação em redes sociais constitui uma das atividades mais populares entre as crianças e os jovens portugueses (Simões, Ponte, Ferreira, Doretto, & Azevedo, 2014). Na adolescência, fase de desenvolvimento caracterizada pela procura de independência relativamente aos pais e pela crescente relevância e influência do grupo de pares, os *media* sociais podem desempenhar um papel muito importante em tarefas de desenvolvimento essenciais e no processo de construção da identidade, que envolvem a compreensão de si próprios e a gestão das relações com os outros, especialmente os pares (Tatsch et al., 2012).

A construção e a gestão de um perfil no *Facebook*, ao envolver a seleção de imagens e de informação a partilhar, a definição de condições de privacidade, a decisão sobre a forma de se apresentar aos outros, sobre quem aceitar no grupo de amigos e com quem partilhar as publicações, constituem oportunidades para a exploração da própria identidade, para o treino das competências sociais e da gestão das relações com os outros. No entanto, e como referem Valkenburg e Peter (2009, 2011), as características da comunicação *online* estão associadas igualmente a alguns riscos, dependendo estes de fatores pessoais, contextuais e tecnológicos.

Na verdade, a comunicação *online* possibilitada pelos mais recentes desenvolvimentos tecnológicos, apresenta características muito particulares, que merecem ser alvo de reflexão, pelos benefícios que podem oferecer, mas igualmente pelos riscos que uma utilização acrítica dos *media* pode acarretar. Entre esses riscos, uma forma de agressão mediada pelas tecnologias digitais, o *cyberbullying*, tem vindo a preocupar, crescentemente, pais, educadores e especialistas das mais diversas áreas disciplinares.

Neste artigo propomos uma breve reflexão sobre as características que diferenciam a comunicação *online* da comunicação face-a-face. Esta reflexão revela-se fundamental para uma compreensão mais aprofundada do contexto comunicacional em que o *cyberbullying* tem vindo a ocorrer, compreensão esta necessária para uma intervenção mais fundamentada. Apresentamos, de seguida, uma caracterização geral do problema do *cyberbullying*, salientando as suas especificidades face ao *bullying* tradicional[2] e fazendo referência ao estado atual da investigação, nomeadamente no que à sua prevalência diz respeito. Sendo desejável que a intervenção privilegie uma dimensão preventiva, pais, escolas, profissionais de diferentes áreas, investigadores e educadores em geral deparam-se com a necessidade de conhecer que medidas são mais eficazes, que abordagens educativas enfatizar, tendo como grande e último objetivo oferecer às crianças e aos jovens um contexto, *offline* e *online*, seguro e favorável ao seu desenvolvimento. Procuraremos deixar aqui algumas sugestões, recorrendo à investigação que tem sido efetuada neste domínio.

2. COMUNICAR NO CIBERESPAÇO

O ciberespaço constitui um contexto privilegiado para a comunicação entre as crianças e os jovens. Assim, é fundamental oferecer-lhes orientações sobre os cuidados a ter no contacto com os outros no ciberespaço e sobre as regras a seguir na interação *online*, e sensibilizá-los para a importância de pautarem o seu comportamento *online* pelos mesmos princípios éticos que orientam a comunicação presencial, e de adotarem cuidados semelhantes quando interagem em redes de contactos e de "amigos" que são, contudo, tendencialmente muito mais amplas do que as redes sociais tradicionais.

A amplitude destas redes não constitui, no entanto, a única particularidade da comunicação no ciberespaço. De facto, a comunicação mediada pelos diversos ecrãs disponíveis apresenta algumas características muito específicas, referidas por diferentes autores (e.g. Amichai-Hamburger, 2007; McKenna, 2015; Willard, 2004), tais como a

2 Utilizamos a designação de *bullying* tradicional, em detrimento de *bullying* presencial ou face-a-face, dado que esta forma de agressão pode ser direta (física e verbal) ou indireta (rumores, exclusão dos grupos, etc.), não implicando, esta última, a presença física do agressor.

invisibilidade/anonimato, a ausência de pistas sociais e contextuais, a instantaneidade na comunicação, a diminuição da importância da aparência física, a oportunidade para o encontro com pessoas que partilham os mesmo gostos, interesses ou problemas, o potencial de mobilização de esforços coletivos, entre outras. Sendo as crianças e os jovens o foco da nossa atenção, importa referir que estas características não são benéficas ou prejudiciais em si mesmas, antes abrem um enorme leque de possibilidades em termos de interação e relações sociais (Matos, 2012).

A (ilusão de) invisibilidade/anonimato possibilitada no ciberespaço constitui uma das características com implicações mais significativas nos nossos comportamentos de comunicação. A literatura refere benefícios associados a um efeito de desinibição que favorece a autoexpressão e a autorrevelação, sobretudo em pessoas mais introvertidas ou com menos competências sociais (Christakis & Fowler, 2010; McKenna, 2015). O contributo para a qualidade das relações interpessoais dos adolescentes, sobretudo no que se refere às relações já existentes, é igualmente evidenciado na investigação (Valkenburg & Peter, 2009, 2011). No entanto, a possibilidade de invisibilidade/anonimato por detrás do ecrã e o efeito de desinibição daí resultante podem favorecer igualmente a manifestação de comportamentos socialmente indesejáveis e que mais dificilmente ocorreriam numa situação de comunicação face-a-face. O ecrã proporciona um sentimento de proteção relativamente a eventuais consequências dos nossos comportamentos e torna também mais difícil antecipar ou prever essas consequências (Willard, 2004).

A compreensão das reações dos outros ao nosso comportamento e do potencial impacto do mesmo é dificultada na comunicação mediada, reduzindo-se, assim, as oportunidades para a empatia, variável que surge, na investigação, associada a menor probabilidade de comportamentos antissociais e de agressão (e.g., Almeida et al., 2012; Gini, Albiero, Benelli, Altoè, 2007). Todas estas características da comunicação *online*, a par de inúmeros e potenciais benefícios podem, assim, favorecer igualmente comportamentos menos desejáveis socialmente, comprometedores da integridade e do bem-estar daqueles que estão do outro lado do ecrã, nomeadamente os comportamentos de *cyberbullying*. Adicionalmente, também do lado de cá do ecrã as consequências negativas podem fazer-se sentir. Para além dos danos que pode provocar nas suas relações

interpessoais, o autor deste tipo de comportamentos fica refém das palavras ou imagens que enviou ou publicou, que se tornam, como refere Boyd (2007), acessíveis a audiências invisíveis, replicáveis e pesquisáveis a longo prazo.

Na comunicação *online* verifica-se, ainda, uma redução das pistas sociais e contextuais (aparência física, gestos, olhar, expressão facial, características do local) que permitem adequar, na comunicação faca-a-face, a comunicação verbal e não-verbal a cada situação e interlocutor e efetuar ajustamentos contínuos a favor de uma maior eficácia da comunicação (Willard, 2004). Por outro lado, essas pistas sociais e contextuais produzem, por vezes, um efeito condicionador ou inibidor da comunicação, devido às expetativas e à pressão social a elas associadas. Assim, no ciberespaço, o menor peso das expetativas e pressões associadas a certas características físicas, sociais ou outras pode ter um efeito facilitador da comunicação (Amichai-Hamburger, 2007; McKenna, 2015).

Uma outra vantagem da comunicação mediada pelas tecnologias apontada pelos autores anteriormente referidos resulta da possibilidade de gestão mais estratégica da comunicação, associada ao facto de a comunicação mediada permitir rever a mensagem que se quer transmitir, não responder de imediato, pensar em qual será a resposta mais desejável e qual a possível reação do recetor. Esta gestão mais estratégica da comunicação permite assim o treino de competências sociais e de comunicação, podendo contribuir para sentimentos de autoestima e de autoeficácia. Por outro lado, a evolução no domínio das tecnologias tem contribuído para aumentar as possibilidades de comunicação em tempo real. Aplicações de mensagens instantâneas são cada vez mais transversais a diferentes equipamentos e *media* sociais (podendo ser instaladas nos dispositivos móveis, como por exemplo o *whatsapp*), permitindo, para além da troca de mensagens de texto, o envio de imagens, a conversação áudio e mesmo a videoconferência. A instantaneidade na comunicação permitida por estas aplicações pode favorecer comportamentos mais impulsivos e irrefletidos, com potenciais consequências negativas nas relações interpessoais.

Depreende-se deste conjunto complexo de características da comunicação *online* que os seus potenciais benefícios e riscos são múltiplos. O conhecimento e a compreensão

dessas características é fundamental para que a balança dos riscos e das oportunidades se desequilibre a favor do desenvolvimento e do bem-estar das crianças e dos jovens, reduzindo as probabilidades de ocorrência de problemas como o *cyberbullying*.

3. *BULLYING* NO CIBERESPAÇO

A ocorrência do *cyberbullying* intensificou-se à medida que as tecnologias da informação e da comunicação se desenvolveram e o seu uso se generalizou, tendo vindo este problema a gerar especial preocupação devido às consequências graves que pode ter, quer nas vítimas, quer nos agressores.

O *cyberbullying* é uma nova forma de *bullying*, perpetrada através de meios eletrónicos ou digitais de comunicação. Nos últimos anos, diversas definições de *cyberbullying* foram propostas pelos investigadores, baseadas na definição e nos critérios utilizados para definir o *bullying* tradicional, adicionando, simultaneamente, novas facetas específicas do *bullying* perpetrado através de dispositivos tecnológicos. Face a essa diversidade, Tokunaga (2010, p. 278) procurou responder às dificuldades conceptuais e operacionais dos investigadores, definindo *cyberbullying* como "qualquer comportamento manifestado através de meios eletrónicos ou digitais por grupos ou indivíduos que, de uma forma reiterada, transmite mensagens agressivas ou hostis com a intenção de fazer mal ou causar incomodidade".

A intenção de provocar danos ou causar incomodidade constitui, desta forma, um critério para a definição de *cyberbullying*, comum ao conceito de *bullying* tradicional. Outras facetas do *bullying* tradicional assumem, no entanto, no caso do *cyberbullying*, novos contornos (Dooley, Pyzalski & Cross, 2009; McGuckin et al., 2012).

A repetição do ato agressivo, característica do *bullying* tradicional, adquire, no caso do *cyberbullying*, um novo significado. Na verdade, a repetição do ato, no *cyberbullying*, pode estar relacionada com o encaminhamento ou visionamento repetido das mensagens hostis, levando a que a vítima experiencie repetidamente a agressão.

Um terceiro critério subjacente à classificação do *bullying* tradicional é o desequilíbrio de poder entre vítimas e agressores que assenta, geralmente, em diferenças em termos de idade e de força física. Este desequilíbrio caracteriza também o *cyberbullying*, embora neste caso o desequilíbrio de poder possa estar relacionado com desiguais competências tecnológicas ou com a situação de fragilidade em que a vítima se encontra, por não saber quem é o autor da agressão e por estar acessível, vinte e quatro horas por dia, sete dias por semana, através da internet e do telemóvel.

Uma outra característica específica do *cyberbullying* é a dimensão da audiência, ampliada infinitamente no ciberespaço, o que contribui para o impacto que este comportamento pode ter nas vítimas.

A investigação em torno do *cyberbullying* permite, ainda, caracterizar este fenómeno relativamente aos meios utilizados para perpetrar a agressão e à natureza dos comportamentos manifestados. No que se refere aos meios utilizados, Smith et al. (2008) referem sete categorias: SMS, MMS, chamadas telefónicas, mensagens de correio eletrónico; salas de conversação (*chatrooms*); mensagens instantâneas e páginas da *Internet*, em que se incluem as redes sociais. A classificação do *cyberbullying* em função da natureza dos comportamentos é diversa na literatura sobre a temática. De acordo com Willard (2007), o *cyberbullying* pode assumir diferentes formas, embora, como refere a autora, algumas destas modalidades de comportamento estejam relacionadas e possam sobrepor-se, o que por vezes dificulta a sua distinção. Constituem exemplos de *cyberbullying* os seguintes comportamentos (Willard, 2007):

- discussão acesa (*flaming*): consiste numa discussão intensa e breve, entre dois ou mais protagonistas, recorrendo a linguagem ofensiva e insultuosa, que tende a ocorrer em espaços públicos de comunicação como os chats, as redes sociais e os jogos *online*;

- assédio (*harassment*): refere-se ao envio repetido de mensagens e/ou imagens ofensivas e insultuosas, através de canais privados de comunicação (como o email e as mensagens instantâneas) ou em espaços de comunicação públicos;

- denigração (*denigration*): consiste em denegrir ou difamar, mediante o envio ou a publicação de informação prejudicial ou falsa, com o objetivo de provocar danos na reputação da vítima;

- usurpação de identidade (*impersonation*): trata-se de enviar ou publicar material fazendo-se passar pela vítima (utilizando passwords e outros dados pessoais), com o objetivo de prejudicar a vítima e comprometer as suas amizades;

- revelação de segredos (*outing*): refere-se ao envio ou à publicação de informação ou imagens de carácter íntimo ou pessoal, com o objetivo de embaraçar ou humilhar a vítima;

- aliciamento (*trickery*): trata-se de persuadir a vítima a revelar informação ou imagens pessoais, visando a sua posterior disseminação ou a sua utilização para a ameaçar;

- exclusão (*exclusion*): consiste em excluir alguém de um grupo ou espaço *online*, como por exemplo os jogos, provocando sentimentos de rejeição;

- ciberperseguição (*cyberstalking*): consiste numa forma de assédio reiterado e particularmente ofensivo ou ameaçador, capaz de provocar sentimentos de medo na vítima.

A investigação desenvolvida até ao presente tem dado um significativo contributo para a compreensão deste fenómeno, não apenas no que se refere às suas características, mas também à sua prevalência. Relativamente à prevalência, a pesquisa produziu resultados de grande diversidade, embora na maioria dos estudos as taxas de vitimização rondem os 10% (McGuckin et al., 2012). Esta diversidade pode estar associada a diversos fatores relacionados com a definição adotada, os meios considerados e a metodologia seguida, nomeadamente no que diz respeito aos instrumentos de medida, à delimitação ou não de um período de tempo nas questões colocadas, às características das amostras, entre outros (Amado & Matos, 2015; Matos, Vieira, Amado, Pessoa, & Martins, 2016; Smith, 2015).

Com o objetivo de proporcionar uma revisão crítica dos estudos realizados, e assim contribuir para ultrapassar a complexidade inerente ao estudo deste fenómeno, têm vindo a ser realizados alguns estudos de revisão e meta-análises. Por exemplo, uma revisão sistemática dos estudos conduzidos nos Estados Unidos, com participantes de idades compreendidas entre os 10 e os 19 anos, levada a cabo por Selkie, Fales e Moreno (2015) revelou que a prevalência do *cyberbullying* variava entre 3% e 72%, enquanto a

prevalência da agressão se encontrava entre 1% e 41%. Uma meta-análise de estudos realizados em diversos países conduzida por Kowalski et al. (2014) sugere que a prevalência do *cyberbullying* se situa entre os 10 e os 40%. Importa ainda referir uma revisão da literatura mais recente, que permitiu a Aboujaoude, Savage, Starcevic e Salame (2015) concluir que a maioria das taxas de *cyberbullying* varia entre os 20% e os 40%.

Em Portugal, diversos estudos foram realizados ao longo dos últimos anos, embora na sua maior parte com amostras de pequena dimensão e restritas em termos geográficos. As taxas de prevalência de vitimização encontradas variam entre os 4.8% e os 29% (Almeida, Correira, Marinho, & Gracia, 2012; Bento, 2011; Campos, 2009; Cruz, 2011; Montalvão, 2015; Ventura, 2011), sendo necessário referir que esta variabilidade pode estar associada aos diferentes períodos de referência utilizados nos diferentes estudos, encontrando-se taxas mais elevadas nos estudos que delimitam um período específico (por exemplo, " Nos últimos 12 meses foste vítima…."), por comparação com os estudos em que se pergunta aos participantes se alguma vez foram vítimas.

Os resultados obtidos no âmbito dos projetos *EU Kids Online* (Livingstone, Haddon, Görzig, & Ólafsson, 2011) e *Net Children Go Mobile* (Mascheroni & Cuman, 2014), desenvolvidos com amostras de maior dimensão constituídas por crianças e jovens com idades entre os 9 e os 16 anos, em diferentes países europeus (25 e 7 países, respetivamente), entre os quais se inclui Portugal, merecem especial atenção, porque sugerem uma tendência para um aumento das situações de *cyberbullying* na Europa, revelando, no caso de Portugal, um aumento das taxas de vitimização de 2% (2010) para 5% (2014).

Um outro estudo, que envolveu 3525 alunos dos 6º, 8º e 11º anos de escolaridade de escolas de diferentes regiões do país, revelou uma prevalência de 7.6% de vítimas e de 3.9% de *bullies* (Matos, Vieira, Amado, Pessoa, & Martins, 2016). Este estudo proporcionou, ainda, informação relevante para a compreensão de diferentes facetas do problema, nomeadamente das estratégias de *coping* a que recorrem as vítimas da agressão. Os dados revelaram que as crianças e os adolescentes vítimas de *cyberbullying* tendem a recorrer mais frequentemente a estratégias tecnológicas de *coping* (tais como

mudar a *password*, bloquear o agressor), uma tendência comum à investigação anterior realizada em diferentes países, embora a eficácia a longo termo deste tipo de estratégias não tenha recebido pouco da investigação (McGuckin et al., 2013).

Outras estratégias mencionadas pelas vítimas consistem em estratégias ativas, traduzindo-se em confrontar o agressor (falar com o agressor e pedir-lhe para parar) e em ter mais cuidado no uso dos *media* digitais. Não fazer nada ou ignorar a agressão são estratégias passivas também muito referidas pelas vítimas (Matos et al., 2016), estando a sua eficácia relacionada com a gravidade e a duração da agressão (Cassidy, Faucher, & Jackson, 2013).

As estratégias sociais de procura de ajuda, consideradas na literatura desejáveis e eficazes, foram também referidas pelas vítimas, que tendem mais frequentemente a pedir ajuda aos amigos (35,9%) do que aos adultos, à semelhança do verificado na investigação anterior (Slonje, Smith, & Frisén 2013; Smith, 2015). Quando recorrem aos adultos, são os pais que surgem em primeiro lugar (27%), sendo a percentagem de vítimas que refere pedir ajuda aos professores bastante inferior (9.3%). Estes dados contrastam com as respostas obtidas junto da amostra total de crianças e adolescentes, quando se lhes perguntou a quem é que as vítimas devem pedir ajuda. Com efeito, 89.7% referiram os pais, 51% os professores e 23.2% os amigos (Matos et al., 2016). Este desfasamento deve suscitar a nossa reflexão, tendo como objetivo propor estratégias que promovam a confiança das crianças e dos jovens nos adultos, e na sua capacidade de os ajudar em situação de vitimização.

Os diferentes estudos referidos anteriormente chamam a atenção para a necessidade de desenvolver esforços no sentido de reduzir as taxas de prevalência do *cyberbullying* e de implementar ações tendentes a capacitar as crianças e os jovens para a prevenção deste tipo de agressão e para saberem como lidar com as situações de *cyberbullying* quando elas ocorrem, no sentido de minimizar o seu impacto negativo. Na verdade, a literatura permite concluir que o *cyberbullying* pode causar grande sofrimento, levando a sentimentos de tristeza, desesperança, raiva e frustração, a problemas de saúde (dores de cabeça, perturbações do sono), a baixa autoestima, refletindo-se também no

contexto escolar, quer na resistência em ir à escola, quer no próprio rendimento académico. Entre as consequências mais graves, foram identificadas situações de comportamentos autodestrutivos e uma maior probabilidade de ideação suicidária, esta última relacionada com vulnerabilidades psicológicas e do contexto familiar (Amado & Matos, 2015; Hinduja & Patchin, 2010; McGuckin et al., 2012).

O *cyberbullying* constitui, assim, um problema que necessita de um contínuo investimento em termos de estudos que contribuam para a sua compreensão, sobretudo tendo em consideração as rápidas transformações no domínio das tecnologias, que trazem, a este fenómeno, facetas continuamente novas. Esta compreensão é fundamental quando se trata de desenvolver iniciativas e projetos tendentes a prevenir a ocorrência do *cyberbullying* ou a minimizar as consequências negativas que este pode ter entre os envolvidos.

4. EDUCAR PARA PROTEGER

A relação das crianças e dos jovens com os *media*, e os potenciais riscos associados ao seu impacto constituíram desde muito cedo motivo de discussão e de preocupação por parte dos pais e educadores em geral e objeto de investigação em diferentes áreas disciplinares. Dos *comics*[3] à rádio, do cinema à televisão, os meios de comunicação desde sempre originaram questões sobre a influência que podem ter no público em geral e, em particular, entre as gerações mais novas (Santos, 2001). A necessidade sentida, em diferentes momentos da evolução dos *media*, de proteger as crianças dos seus potenciais efeitos nocivos foi acompanhada por um desenvolvimento paralelo de diferentes conceções sobre a perspetiva a adotar em termos de intervenção, nomeadamente no que se refere ao papel da educação. Assim, na primeira metade do século XX, enquadrada num modelo teórico que concebia os meios de comunicação de massas como omnipotentes e tendo um efeito direto na audiência (Santos, 2001), preponderou uma perspetiva assente numa conceção da criança como indefesa, com pouca capacidade crítica e a necessitar de proteção, a que correspondeu uma atitude educativa protecionista

3 Termo utilizado para designar as bandas desenhadas nos Estados Unidos.

(Gonnet, 2007). De acordo com esta perspetiva, as crianças precisariam de ser protegidas dos efeitos nocivos diretos e imediatos dos meios de comunicação. Apesar dos desenvolvimentos que a investigação em torno do impacto dos *media* sentiu, sobretudo a partir dos anos 60 e até à atualidade, a verdade é que esta atitude protecionista tende a ressurgir, sobretudo em momentos em que o aparecimento de novos *media* origina novos (ou velhos) receios, questões, e preocupações. A rápida evolução das tecnologias digitais, que progressivamente suportam a generalidade dos *media* que existem na atualidade, e a utilização crescente da Internet pelas crianças e pelos jovens, mais recentemente através dos dispositivos móveis, constitui um desses momentos, em que o risco de adotar uma atitude protecionista se renova.

No entanto, a evolução na forma de entender a influência dos *media* tem revelado a complexidade da relação dos *media* com uma audiência que apresenta características particulares, se move em contextos familiares e sociais diferenciados e cuja preparação para a utilização dos *media* pode situar-se e mover-se ao longo de múltiplos pontos de um continuum que representa a literacia mediática. A pergunta sobre se os *media* têm ou não efeitos nocivos tem vindo então a ser substituída pela pergunta "De que modo, e em que medida, os *media* contribuem, se contribuem, como um entre diversos fatores que, em combinação, explicam o fenómeno social em causa?" (Livingstone, 2007, p. 11).

Entre os diversos fatores que interagem nesta complexa relação dos *media* com os cidadãos, e no caso específico da nossa reflexão, com as crianças e os jovens, a educação, em diferentes contextos (familiares, de educação formal e não formal) tem vindo a merecer especial atenção, com o objetivo de minorar os riscos associados ao uso dos *media* e de simultaneamente potenciar os benefícios que estes podem trazer ao desenvolvimento das crianças e dos jovens.

Estamos pois a referir-nos a uma outra perspetiva educativa, que visa capacitar as crianças e os jovens para uma utilização dos *media* que seja eficaz, segura e responsável individual e socialmente. Esta perspetiva capacitadora assenta no princípio de que as crianças podem desenvolver atitudes e práticas ativas, responsáveis e críticas, sendo

fundamental uma intervenção educativa destinada a promover esse desenvolvimento (Pinto et al., 2011).

É neste enquadramento conceptual que integramos a nossa reflexão sobre a proteção das crianças e dos jovens no ciberespaço, alicerçada na convicção de que a educação, nomeadamente a educação mediática, constitui a melhor forma de as proteger, na medida em que seja capaz de promover as suas competências de literacia mediática e digital.

Com efeito, uma atitude protecionista, assente na proibição e no controlo, envolve também alguns riscos. Sendo a Internet e o telemóvel tão importantes na vida das crianças e dos jovens, a proibição ou restrições em termos de acesso e de uso contribuiriam para criar um desfasamento entre os adultos, a cultura escolar e as experiências de vida diárias dos mais novos, que são largamente mediadas pelas tecnologias, para além de que lhes transmitiria a ideia de que os adultos não conhecem e não compreendem o seu mundo (Matos, Festas, & Seixas, 2016). A este propósito é pertinente referir a opinião de uma adolescente de 16 anos, recolhida no âmbito de um estudo desenvolvido por Stald (2008) sobre o significado do telemóvel na vida dos jovens, segundo a qual os pais geralmente desconhecem a importância que o telemóvel tem vindo a assumir na sua vida. Este desconhecimento, refere a adolescente, está associado ao facto de os pais considerarem, sobretudo, a função de comunicação do telemóvel, negligenciando o significado social que o mesmo adquiriu para os jovens, significado associado às suas experiências e contextos de uso.

A compreensão do significado social que os *media* digitais têm para as gerações mais novas constitui um primeiro passo para que os pais, os professores e outros educadores sejam capazes de exercer o seu papel mediador, na relação das crianças e dos jovens com os *media* e os seus conteúdos. De facto, os estudos que procuraram compreender as razões que levam as vítimas de *cyberbullying* a pedir ajuda mais frequentemente aos amigos, do que aos adultos revelam que, entre as razões indicadas pelos participantes, o medo de que lhes seja retirado o telemóvel ou o acesso à Internet surge como uma das mais referidas (Cassidy, Faucher, & Cassidy, 2013; Willard, 2007),

dados que evidenciam, precisamente, a importância que os *media* têm, atualmente, na vida das crianças e dos jovens.

Em alternativa a uma atitude protecionista assente na restrição e na proibição, os pais, professores e educadores em geral podem desenvolver esforços, de preferência concertados, no sentido de promover, nas crianças e jovens, competências para uma utilização ativa, crítica e responsável do ciberespaço, competências relacionadas com os três papéis que eles desempenham enquanto comunicadores: (1) recetores, (2) criadores e emissores de mensagens e de textos mediáticos e (3) observadores/espetadores da comunicação que ocorre em locais mais ou menos públicos, mais ou menos privados do ciberespaço. Em todos estes papéis é possível correr riscos, sobretudo se forem desempenhados sem preparação, sem uma formação que permita o conhecimento e promova a reflexão sobre as características da comunicação nesses espaços, e sobre as responsabilidades e os direitos que estão associados a esses três diferentes papéis.

5. EDUCAR PARA PROTEGER "*COMUNICADORES NÓMADAS*" [4]

Os desenvolvimentos tecnológicos mais recentes, no que se refere aos dispositivos móveis e às crescentes potencialidades que os mesmos oferecem em termos de instantaneidade na comunicação e acesso à Internet em qualquer lugar, vêm colocar grandes e novos desafios aos pais, escolas e educadores em geral. Com efeito, estratégias tradicionais de supervisão e acompanhamento das crianças e dos jovens, na sua utilização dos *media*, tais como a colocação do computador num espaço comum da casa, perdem utilidade e eficácia, quando eles levam a Internet no bolso, para onde quer que vão.

Na verdade, a convergência de diferentes ferramentas de comunicação numa mesma plataforma, e o uso generalizado (ver crianças) dos dispositivos móveis como o

4 Designação utilizada por Pérez-Tornero e Varis (2010, p. 38) para se referirem aos utilizadores multimédia, que fazem um uso combinado dos velhos e dos novos *media*, transportando-os consigo numa espécie de "bolha" pessoal, o que lhes permite comunicar de qualquer lugar e em qualquer momento.

smartphone e o *tablet* para aceder à Internet, em particular às redes sociais, requerem uma reflexão profunda sobre as estratégias de mediação da relação dos mais novos com os *media* digitais e sobre os próprios objetivos que devem nortear a mediação e a educação. Destacamos, neste âmbito, o importante papel dos pais, mas também o papel da escola, nomeadamente no que se refere à educação para um uso esclarecido, crítico, e seguro dos *media* digitais.

As vantagens da mediação parental foram realçadas em diversos estudos, nomeadamente aqueles que se debruçaram sobre a influência da televisão nas atitudes e comportamentos das crianças. Esses estudos demonstraram o potencial de diferentes estratégias mediadoras, enquanto fatores protetores de eventuais riscos associados à utilização dos *media* pelos filhos (Matos, 2006).

No que diz respeito à Internet, a investigação sobre a mediação parental, entendida como os comportamentos dos pais que visam proteger os filhos dos riscos e perigos *online* (Livingstone, 2007), tem produzido resultados variáveis em função das formas de mediação consideradas. A mediação restritiva, assente no estabelecimento unilateral de regras em termos de tempo e de conteúdo ou no recurso a *software* de controlo, surge na investigação associada a uma maior exposição das crianças a riscos *online*. Pelo contrário, estratégias de mediação ativa, que consistem em estabelecer regras com base na discussão e na explicação, em conversar com os filhos sobre os riscos *online* e a segurança na Internet surge associada a menor exposição a riscos *online*, incluindo o *cyberbullying* (Mesch, 2009; Sasson & Mech, 2014). A coesão e o apoio familiar surgem igualmente na investigação como fatores protetores da exposição a riscos *online* e do *cyberbullying* (Martins, Simão, Freire, Caetano, & Matos, 2016; Sasson & Mesch, 2014).

Podemos depreender que os resultados da investigação sugerem que as estratégias de mediação mais eficazes são aquelas que assentam numa relação de proximidade e de diálogo, apelam à responsabilização e têm como grande objetivo promover a autonomia das crianças e dos jovens na sua relação com os *media* digitais. Tendo em consideração o crescente protagonismo dos dispositivos móveis, serão essas as estratégias e os objetivos que nos parecem mais promissores, em termos de capacitação das crianças e

dos jovens para um uso esclarecido, eficaz, seguro e responsável de equipamentos e de ferramentas de comunicação que transportam consigo, quando saem de casa.

A par da família, a escola desempenha um papel extremamente importante e indispensável neste âmbito[5], cabendo-lhe responsabilidades particulares no que se refere à promoção da literacia mediática e da cidadania digital dos alunos. São várias as linhas de ação que a escola pode adotar com o objetivo de desenvolver, nos alunos, atitudes e comportamentos críticos e responsáveis relativamente aos *media*. Destacamos as iniciativas de educação mediática[6], destinadas a ajudar os alunos a "desenvolver hábitos de questionamento e competências de expressão de que precisam para serem pensadores críticos, comunicadores eficazes e cidadãos ativos no mundo atual" (Scheibe & Rogow, 2012, p. 211).

Neste âmbito, podem ser abordadas as características da comunicação mediada pelas tecnologias e temas como a segurança *online*, a privacidade, a netiqueta, bem como os riscos envolvidos na utilização dos *media* digitais, nomeadamente o contacto com conteúdos indesejáveis (racismo, xenofobia, conteúdos de cariz sexual ou que apelam à algum tipo de discriminação) ou riscos associados a comportamentos prejudiciais que lesam a integridade de terceiros, tais como o *cyberbullying*. Pode ainda ser promovida a reflexão dos alunos sobre o seu duplo papel, de emissores e de recetores, e sobre os princípios éticos sobre os quais devem alicerçar os seus comportamentos de comunicação.

Além de recetores e emissores, as crianças e os jovens são hoje observadores/espetadores da comunicação que se estabelece no ciberespaço, e este terceiro papel traz consigo inerentes e não menos importantes responsabilidades, que merecem ser alvo de reflexão, como aliás tem vindo a ser realçado na literatura sobre o *cyberbullying* (Cassidy et al., 2013; Seixas, Fernandes, & Morais, 2016). Os observadores de situações de *cyberbullying* desempenham um papel que pode ser determinante, capaz de contribuir para perpetuar a agressão (quando por inação se é cúmplice da agressão) ou

5 Para uma abordagem mais aprofundada do papel da escola na prevenção do *cyberbullying*, consultar Matos e Seixas (2016).
6 A educação para os *media* constitui uma das áreas temáticas que integram a área curricular de educação para a cidadania no ensino pré-escolar, básico e secundário.

para interromper o processo de vitimização (quando se denuncia a situação, quando se apoia a vítima ou se demonstra desaprovação em relação aos comportamentos agressivos). A formação dos alunos para que, enquanto observadores, ajudem a combater o *cyberbullying* é, desta forma, fundamental (Matos & Seixas, 2016).

A abordagem do *cyberbullying* em campanhas de sensibilização, em ações de formação de alunos, professores e outros membros da comunidade educativa, e mesmo o tratamento desta temática em sala de aula é recomendada por diversos autores, que salientam a importância de sensibilizar toda a comunidade educativa e de favorecer o desenvolvimento de uma conceção comum acerca deste problema, necessária a uma identificação precoce e a uma intervenção mais eficaz.

A abordagem deste tema na escola é ainda fundamental para desenvolver uma cultura escolar que desaprova o *cyberbullying*. A importância crescente que os pares adquirem na transição da infância para a adolescência torna os adolescentes mais suscetíveis à sua influência. Estudos anteriores sugerem, precisamente, que a opinião de pessoas significativas constitui um bom preditor das intenções dos adolescentes de perpetrarem *cyberbullying*, e que aqueles que percecionam uma pressão social negativa relativamente a este tipo de comportamentos demonstram menor intenção de os manifestar (Heirman & Walrave, 2012). Tendo estas conclusões em consideração, o desenvolvimento de iniciativas de sensibilização e de formação na escola, tendentes a criar, nos alunos, atitudes de desaprovação do *cyberbullying*, poderão ter um feito dissuasor da manifestação deste tipo de comportamentos.

Uma outra forma de a escola contribuir para a educação dos alunos no que se refere à sua relação com os *media* consiste em adotar uma atitude pró-ativa e positiva, integrando as TIC em atividades a desenvolver dentro e fora da sala de aula, envolvendo os alunos, os professores e outros membros da escola, e mesmo os pais. A promoção de uma utilização positiva das TIC constitui uma estratégia de prevenção dos seus potenciais efeitos nocivos, para além de que gera proximidade com o mundo dos alunos e favorece a criação de um ambiente em que eles se sentem confortáveis para falar das suas experiências no ciberespaço, sejam elas positivas ou negativas.

6. CONCLUSÃO

A relação das crianças e dos jovens com os *media* digitais foi alvo de múltiplos estudos ao longo dos últimos anos, estudos que têm contribuído para a caracterização dos hábitos de utilização destes *media*, bem como para a identificação e a compreensão dos benefícios e dos potencias riscos decorrentes do seu uso. Entre os vários temas objeto de investigação, a problemática do *cyberbullying* continua a inspirar numerosos investigadores em todo o mundo, numa tentativa de proporcionar uma caracterização ampla e compreensiva de um fenómeno que pode ter uma forte impacto e causar grande sofrimento nas vítimas.

Constituindo uma forma de *bullying*, o *cyberbullying* apresenta, no entanto, características muito particulares, cuja compreensão é essencial para que se possa desenvolver estratégias de prevenção e de intervenção eficazes. Algumas dessas características decorrem da natureza da própria comunicação no ciberespaço, que possibilita o anonimato, coloca as vítimas numa situação de acessibilidade permanente e permite a formação de audiências invisíveis e de dimensão infinita (Nocentini et al., 2010; Slonje & Smith, 2008). Neste artigo, procurámos apresentar uma caracterização sucinta deste problema, enquadrando-o num contexto de comunicação que assume, continuamente, novas facetas, resultado de uma evolução tecnológica que desafia a sociedade em geral, e muito em particular, todos aqueles que têm responsabilidades educativas.

Neste contexto, a necessidade de proteger as crianças e os jovens é sentida com particular preocupação, para a qual concorre a menor familiaridade dos adultos em relação aos novos *media* e a mediatização de casos em que crianças e jovens se veem envolvidos em situações de risco. A investigação desenvolvida sobre os riscos do ciberespaço, nomeadamente os estudos em torno da problemática do *cyberbullying*, tem revelado a importância de desenvolver esforços em diferentes contextos (familiares, escolares, associativos, de educação não formal), com o objetivo de educar as crianças e os jovens para uma utilização esclarecida, crítica, segura e responsável dos *media* digitais. No entanto, os mais recentes desenvolvimentos no que se refere às potencialidades dos

dispositivos móveis acrescentam complexidade a uma tarefa já difícil, e desafiam crescentemente os adultos e as suas estratégias tradicionais de supervisão, de acompanhamento e de mediação. É neste contexto que a educação de crianças e jovens para a *autonomia crítica*[7] no uso dos *media* digitais se assume como uma estratégia privilegiada de proteção.

7 Expressão utilizada por Masterman (1985) para se referir ao que o autor considera ser um dos principais objetivos da educação mediática e uma das mais importantes e difíceis tarefas dos professores que trabalham neste domínio.

7. REFERÊNCIAS

Aboujaoude, E., Savage, M. W., Starcevic, V., & Salame, W. O. (2015). Cyberbullying: Review of an old problem gone viral. *Journal of Adolescent Health, 57*, 10-18.

Almeida, A., Correia, I., Marinho, S., & Garcia, D'J. (2012). Virtual but not less real: A study of cyberbullying and its relations to moral disengagement and empathy. In Q. Li, D. Cross, & P. K. Smith (Eds.), *Cyberbullying in the global playground: Research from international perspectives* (pp. 223-244). Oxford: Wiley-Blackwel.

Amado, J., & Matos, A. (2015). O cyberbullying entre os comportamentos de risco online. In G. L. Miranda (Org.), *Psicologia dos comportamentos online* (pp. 81-105). Lisboa: Relógio d'Água Editores.

Amichai-Hamburger, Y. (2007). Personality, individual differences and internet use. In A. Joinson, K. McKenna, T. Postmes, & U-D Reips (Eds.), *The Oxford handbook of internet psychology* (pp. 204-221). New York: Oxford University Press.

Bento, A. M. M. S. (2011). O cyberbullying no contexto português. (Tese de mestrado, Universidade da Beira Interior). Consultado em https://ubibliorum.ubi.pt/bitstream/10400.6/2735/1/Cyberbullying%20no%20Contexto%20Portugu%C3%AAs.pdf

Boyd, D. (2008). Why youth social network sites: The role of networked publics in teenage social life. In D. Buckingham (Ed.), *Youth, identity, and digital media*. *The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning* (pp. 143-164). Cambridge, MA: The MIT Press.

Campos, M. (2009). Cyberbullying. Natureza e ocorrência em contexto português (Tese de mestrado, ISCTE). Consultado em https://repositorio.iscte-iul.pt/handle/10071/1884

Cassidy, W., Faucher C., & Jackson M. (2013). Cyberbullying among youth: A comprehensive review of current international research and its implications and application to policy and practice. *School Psychology International, 34*(6), 575–612. doi: 10.1177/0143034313479697.

Christakis, N., & Fowler, J. (2010). *Conectados* (Trad. Por A. Diéguez, L. Vidal & E. Schmid). Madrid: Santillana Ediciones Generales.

Cloutier, J. (1975). *A era de Emerec ou a comunicação audio-scripto-visual na hora dos self-media*. Lisboa: ITE.

Cruz, A. C. C. (2011). O cyberbullying no contexto português. (Tese de mestrado, Universidade Nova de Lisboa). Consultado em http://www.fcsh.unl.pt/eukidsonline/docs/disserta%C3%A7ao%20mestrado%20cyberbullying.pdf

Dooley, J. J., Pyzalski, J., & Cross, D. (2009). Cyberbullying Versus Face-to-Face Bullying: A Theoretical and Conceptual Review. *Zeitschrift für Psychologie/Journal of Psychology*, *217*(4), 182-188.

Garaigordobil, M. (2015). Cyberbullying in adolescents and youth in the Basque Country: Prevalence of cybervictims, cyberaggressors, and cyberobservers. *Journal of Youth Studies*, *18*(5), 569-582. doi: 10.1080/13676261.2014.992324

Gini, G., Albiero, P., Benelli, B., & Altoè, G. (2007). Does empathy predict adolescents' bullying and defending behavior?, *Aggressive Behavior, 33*, 467–476.

Gonnet, J. (2007). *Educação para os media: As controvérsias profundas*. Porto: Porto Editora.

Heirman, W., & Walrave, M. (2012). Predicting adolescent perpetration in cyberbullying: An application of the theory of planned behaviour. *Psicothema*, *24*(4), 614-620. Consultado em http://www.psicothema.es/pdf/4062.pdf**.**

Hinduja, S., & Patchin, J. W. (2010). Bullying, Cyberbullying, and Suicide. *Archives of Suicide Research*, *14*(3), 206-221. Consultado em https://legacy.touro.edu/EDGRAD/EAC/docs/Hinduja_Article_2010.pdf

Instituto Nacional de Estatística. (2016). Sociedade da Informação e do Conhecimento. Inquérito à Utilização de Tecnologias da Informação e da Comunicação pelas Famílias. Consultado em https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=250254698&DESTAQUESmodo=2

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin*, *140*, 1073–137.

Livingstone, S. (2007). Do the media harm children?: Reflections on new approaches to an old problem. *Journal of children and media*, *1*(1). 5-14. doi: 10.1080/17482790601005009

Livingstone, S. (2007). Strategies of parental regulation in the media rich home. *Computers and Human Behavior*, *23*, 920-941.

Livingstone, S., Haddon, L., Görzig, A., & Ólafsson K. (2011). *Risks and safety on the internet: The perspective of European children*. *Full Findings*. LSE, London: EU Kids Online.

Martins, M. J. D., Simão, A. M. V., Freire, I., Caetano, A. P., & Matos, A. (2016). Cyber-victimization and cyber-aggression among Portuguese adolescents: The relation to family support and family rules. *The International Journal of Cyber Behavior, Psychology and Learning*, *6*(3), 65-78. DOI: 10.4018/IJCBPL.2016070105

Mascheroni, G., & Cuman, A. (2014). *Net Children Go Mobile: Final report. Deliverables D6.4 & D5.2*. Milano: Educatt. Consultado em http://www.netchildrengomobile.eu/reports/

Masterman, L. (1985). *Teaching the media*. London: Routledge.

Matos, A. P. M. (2006). *Televisão e violência. (Para) Novas formas de olhar*. Coimbra: Almedina.

Matos, A. (2012). A nova midia: Desafios sociais e educativos. In N. Baldin & C. Albuquerque (Orgs.), *Novos desafios na educação: Responsabilidade social, democracia e sustentabilidade* (pp. 123-143). Brasília: Editora LiberLivro.

Matos, A. P. M., Festas, M. I., & Seixas, A. M. (2016). Digital media and the challenges for media education. *Applied Technologies and Innovations,* 12(2), 43-53, http://dx.doi.org/10.15208/ati.2016.04. Consultado em https://academicpublishingplatforms.com/article.php?journal=ATI&number=20&article=2287

Matos, A., & Seixas, A. M. (2016). How schools can prevent, detect and handle cyber bullying. In O. Samnoen (Ed.). *Children, teenagers and cyber bullying: A guidebook for parents and schools* (pp. 40-54). Ankara: Hakan SAKA (Tasarımedya Reklam), T.C. The Ministry of Culture and Tourism, General

Directorate of Libraries and Publications. Consultado em http://www.becybersafe.org/catalogue/index.pdf

Matos, A. P. M., Vieira, C. C., Amado, J., Pessoa, T., & Martins, M. J. D. (2016). Cyberbullying in Portuguese schools: Prevalence and characteristics, *Journal of School Violence*. doi: 10.1080/15388220.2016.1263796

Nocentini, A., Calmaestra, J., Schultze-Krumbholz, A., Scheithauer, H., Ortega, R., & Menesini, E. (2010). Cyberbullying: Labels, behaviours and definition in three European countries. *Australian Journal of Guidance & Counselling*, *10*(2), 129-142. doi**:** http://dx.doi.org/10.1375/ajgc.20.2.129

McGuckin, C., Corcoran, L., Crowley, N., O'Moore, M., Calmaestra, J., Del Rey, R., … Mora-Merchán, J. A. (2012). Introdução ao cyberbullying. In T. Jäger, C. Stelter, J. Amado, A. Matos, & T. Pessoa (Eds.), *Cyberbullying - Um manual de formação de pais* (pp. 78-123). Consultado em http://ct4p.zepf.eu/CT4P_Training_manual_PT.pdf

McGuckin, C., Perren, S., Corcoran, L., Cowie, H., Dehue, F., Ševčíková, A., … Völlink, T. (2013). Coping with cyberbullying: How can we prevent cyberbullying and how victims can cope with it. In P. K. Smith & G. Steffgen (Eds.), *Cyberbullying through the new media: Findings from an international network* (pp. 121-135). East Sussex: Psychology Press.

McKenna, K. (2015). Do outro lado do espelho da Internet. Exprimir e validar o 'verdadeiro eu'. In G. L. Miranda (Org.), *Psicologia dos comportamentos online* (pp. 195-226). Lisboa: Relógio d'Água Editores.

McLuhan, M. (1964). *Understanding media: The extensions of man*. New York: McGraw-Hill.

Mesch, G. (2009). Parental mediation, online activities, and cyberbullying. *Cyberpsychology and Behavior*, *12*(4), 387-393. doi: 10.1089/cpb.2009.0068.

Montalvão, N. M. M. (2015). Cyberbullying: Caracterização do fenómeno em Portugal. (Tese de mestrado, Universidade do Minho). Consultado em https://repositorium.sdum.uminho.pt/bitstream/1822/40722/1/Nuno%20Manuel%20Martins%20Montalv%C3%A3o.pdf

Pérez Tornero, J. M., & Varis, T. (2010). *Media literacy and new humanism*. Moscow: UNESCO. Consultado em http://unesdoc.unesco.org/images/0019/001921/192134e.pdf.

Pinto, M. (Coord.), Pereira, S., Pereira, L., & Ferreira, T. D. (2011). *Educação para os media em Portugal: Experiências, atores e contextos.* Lisboa: Entidade Reguladora para a Comunicação Social/CECS, Universidade do Minho.

Santos, J. R. (2001). *Comunicação*. Lisboa: Prefácio.

Sasson, H., & Mesch, G. S. (2014). Parental mediation, peer norms and risky online behaviors among adolescents. *Computers in Human Behavior*, *33*, 32-38.

Scheibe, C., & Rogow, F. (2012). *The teacher's guide to media literacy: Critical thinking in a multimedia world*. Thousand Oaks, California: Corwin.

Seixas, S., Fernandes, L., & Morais, T. (2016. *Cyberbullying: Um guia para pais e educadores*. Lisboa: Plátano Editora.

Selkie, E. M., Fales, J. L., & Moreno, M. A. (2016). Cyberbullying prevalence among US middle and high school-aged adolescents: A systematic review and quality assessment. *Journal of Adolescent Health, 58*, 125-133. doi: 10.1016/j.jadohealth.2015.09.026

Simões, J. A., Ponte, C., Ferreira, E., Doretto, J., & Azevedo, C. (2014). *Crianças e meios digitais móveis em Portugal. Resultados nacionais do projeto Net Children Go Mobile*. Lisboa, Portugal: CesNova - FCSH/UNL.

Slonje, R., Smith, P. K., & Frisén, A. (2013). The nature of cyberbullying, and strategies for prevention. *Computers in Human Behavior*, *29*, 26–32. doi:10.1016/j.chb.2012.05.024

Smith, P. K. (2015). The nature of cyberbullying and what we can do about it. *Journal of Research in Special Educational Needs*, *15*(3), 176-184. doi: 10.1111/1471-3802.12114

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett N. (2008). Cyberbullying, its forms and impact on secondary school pupils. *Journal of Child Psychology and Psychiatry*, *49*(4), 376-385. doi:10.1111/j.1469-7610.2007.01846.x.

Stald, G. (2008). Mobile identity: Youth, identity, and mobile communication media. In D. Buckingham (Ed.), *Youth, identity, and digital media*. *The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning* (pp. 143-164). Cambridge, MA: The MIT Press. doi: 10.1162/dmal.9780262524834.143

Tatsch, I., Kimmel, B., Borries, E., Rack, S., Jäger, T., & Samnøen, Ø. (2012). Introdução aos novos meios de comunicação. In Jäger, T., Stelter, C., Amado, J., Matos, A., & Pessoa, T. (Eds), Cyberbullying - Um manual de formação de pais. Consultado em http://ct4p.zepf.eu/CT4P_Training_manual_PT.pdf

Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behaviour*, *26*, 277-287. doi:10.1016/j.chb.2009.11.014.

Valkenburg P. M., & Peter, J. (**2009).** Social consequences of the Internet for adolescents: A decade of research. *Current Directions in Psychological Science*, *18*(1), **1-5.** doi: 10.1111/j.1467-8721.2009.01595.x.

Valkenburg, P. M., & Peter, J. (**2011).** Online communication among adolescents: An integrated model of its attraction, opportunities, and risks. *Journal of Adolescent Health*, *48*, 121–127. doi:10.1016/j.jadohealth.2010.08.020.

Ventura, P. (2011). *Incidência e impacto do "cyberbullying" nos alunos do terceiro ciclo do ensino básico português*. Granada, Espanha: Editorial de la Universidad de Granada.

Willard, N. (2004). *I Can't See You – You Can't See Me - How The Use Of Information And Communication Technologies Can Impact Responsible Behavior*. Consultado em Http://Www.Essex.Org/Vertical/Sites/%7B60B9D552-E088-4553-92E3-EA2E9791E5A5%7D/Uploads/%7B45A3F14B-D336-4006-83EB-4FDDED8D5D0D%7D.PDF

Willard, N. E. (2007). *Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress*. Champaign, IL: Research Press.

CYBERLAW
by CIJIC

COMO PROTEGER AS CRIANÇAS DOS CONTEÚDOS DISPONÍVEIS NA INTERNET?

HOW TO PROTECT CHILDREN FROM CONTENT AVAILABLE ON THE INTERNET?

HUGO CUNHA LANÇA [1]

1 Instituto Politécnico de Beja. Correio eletrónico: hdlanca@gmail.com

RESUMO

Este texto tem como objetivo responder a uma única questão: como proteger as crianças dos conteúdos disponíveis na internet. Questão prejudicial foi densificar os conceitos de criança e de proteção, para que a tese se possa construir sobre uma base sólida. Como foi fundamental uma análise crítica aos perigos a que as crianças são expostas, de forma a desconstruir fábulas e mitos que têm servido para fomentar o pânico nos educadores e formado uma tempestade perfeita para a intervenção estadual.

Partindo da constatação que existem conteúdos ilegais e conteúdos que, apesar de legais, podem ser lesivos para as crianças, subscrevo que os Estados apenas devem regular diretamente os primeiros, quer através da Lei, quer através de mecanismos de cooperação internacional, dada a globalidade da internet. No que concerne aos conteúdos lesivos, defendo uma abordagem holística repartida entre a obrigação dos pais (e outros educadores) de protegerem os seus filhos, a responsabilização dos fornecedores de conteúdos e dos prestadores de serviço em linha, não apenas numa dimensão punitiva, mas, sobretudo, numa aceção preventiva, pelo recurso a códigos de conduta, regulação normativa e regulação através do código.

Palavras-Chave: Criança; Proteção; Internet; Corregulação

ABSTRACT

This article aims to provide an answer to a single question: how to protect children from content available on the internet. The crucial question was to densify the concepts of 'child' and 'protection', so that the thesis may be built on a solid basis. Surely, a critical analysis on the hazards children are exposed to was essential in order to dispel rumors and myths that have been encouraging panic amongst educators and ushering in a perfect storm for State intervention.

The conviction that State regulation is carried out directly and indirectly raised the need to determine the responsibility of the State, parents, content providers, and online services providers, as only through co-regulation will it be possible to develop a child-friendly telematic environment. Based on the assumption that illegal content exists and content that, though illegal, may be harmful for children, we assert that States should only regulate the former, whether by Law or by international cooperation mechanisms, given the universal character of the internet. Vis-à-vis hazardous content, we advocate a holistic approach broken up between parents' obligations (and other educators') to protect their children, the accountability of online services providers, not only in a punitive dimension, but mainly in a preventive capacity, through the use of codes of conduct, normative regulation and regulation through the code.

Keywords: Children; Protection; Internet; Co-Regulation

1. INTRODUÇÃO

"Imagine o surgimento de uma nova tecnologia de comunicação. Com esta ferramenta é possível interagir com qualquer pessoa localizada em qualquer parte do mundo, desde que a outra pessoa disponha do mesmo *hardware*. Pode manter-se informado, expressar-se de uma maneira nunca antes imaginável e ter acesso a todo o conhecimento já registado pela humanidade. Esta tecnologia muda a educação, o trabalho, a vida familiar, o entretenimento, a política e a economia. Ainda assim, é bastante simples. As crianças, de facto, vão ter mais facilidade que os adultos para aprender a usá-la. Quando se habituar a esta tecnologia, vai perguntar-se como conseguiu viver sem ela. Nenhuma pessoa inventou este modo de comunicar. Em vez disso, este desenvolveu-se espontânea e coletivamente ao longo do tempo. E, hoje, nenhuma entidade é dona dele ou pode controlá-lo, mas este funciona muito bem. Surpreendentemente, esta tecnologia tem milhares de anos. É o alfabeto"[1].

Servem estas primeiras linhas para limitar o entusiasmo deste que vos escreve: depois de meses e meses de leituras diárias sobre *o admirável mundo novo* da internet[2],

1 SHAPIRO, Andrew L. - *The Disappearance of Cyberspace and the Rise of Code*. [Em linha]. Cambridge: Harvard University. [Consult. 13 Maio 2013]. Disponível em: http://cyber.law.harvard.edu/works/shapiro/Disappearance.pdf<, p. 1 [trad. nossa].

2 A expressão corresponde à abreviatura de *Interconnected Networks* ou de *Internetwork Systems*. Internet com "i" minúsculo; não o faço pelo prazer de ser iconoclasta, nem sei se sou pioneiro [porque não sou obstinado em ser original], mas, por certo que, sou dos primeiros investigadores, que se debruçaram sobre a temática, a escrever a locução com minúscula; e não o fiz por imperativos gramaticais [até porque não desconheço que a questão é controvertida nos melhores dicionários e autores de grande coturno veementemente incitam a usar a maiúscula], mas porque a desmistificação do conceito de internet é parte estruturante das minhas reflexões. Dessarte, utilizo o vocábulo "internet" como nome comum (pelo que o "i" inicial é minúsculo) e como uma palavra portuguesa, não como estrangeirismo, o que exigiria itálico. A segunda premissa é mais simples: a palavra está de tal forma arreigada no nosso léxico que é, hoje, uma realidade da nossa língua; no que concerne à primeira, não apenas a locução é a redução do nome comum inglês *supra* mencionado, como, entendo que, a internet, hoje, não pode continuar a ser interpretada como uma entidade una, mas como um conjunto de muitas redes interligadas, através de protocolos comuns, com regras e filosofias próprias e heterogéneas; porque a internet é a *world wide web*, mas também é, *inter alia*, o correio eletrónico, a *voice-over-internet protocol*, o *streaming*, o compartilhamento de arquivos, o acesso remoto, díspares realidades, que suscitam diferentes questões e problemas, pelo que, estou em crer, a palavra deve qualificar-se como nome comum e não como nome próprio. Ao que acresce o mais importante: a imperatividade de interpretar a rede como ela realmente é, não sucumbindo a efabulações. A internet pode ser a concretização não distópica de um maravilhoso mundo novo mas, no final do dia, é tão somente um novo meio de comunicação; se escrevemos televisão, rádio, telégrafo, jornal com inicial minúscula, insistir em escrever internet com maiúscula é endeusar uma realidade que, não obstante a sua colossal importância, é profana.

há o premente risco de me perder no arrebatamento das minhas diásporas e interpretar a internet como o *novo iluminismo* e construir as minhas teses com base em hipérboles vazias, na decetiva premissa de que a internet é mais transcendente do que na realidade é!

É axiomático que a internet é um elemento nuclear da modernidade. Mas, recordo, quando Florentino Ariza entregou a sua vida à muito nobre atividade de telegrafista, decisão que moldou a sua vida e lhe permitiu conhecer Fermina Daza, cuja distância lhe fez companhia toda a sua vida, fê-lo porque, tal como os seus contemporâneos, estava imbuído da certeza certa de que o telégrafo iria mudar o mundo para sempre! A invenção do telégrafo, interpretada como *uma grande obra de Deus*, foi, depois de inúmeras outras, a primeira grande inovação técnica que [alegadamente] transformou, de modo indelével a vida social, numa obsessão pela modernidade, que nos rouba a lucidez e nos faz esquecer que "a invenção da imprensa, conquanto engenhosa, comparada com a invenção das letras é coisa de somenos importância"[3].

Dessarte, nas suas multivalências, a internet é, sobretudo, um meio de comunicação! Imponente, que nos esmaga, mas, enfatizo, é apenas um novo meio de comunicação, como antes foram as torres persas, o alfabeto, a impressão, o telégrafo, o comboio, o correio, o telefone, a rádio e a televisão, premissa que, como uma marca de água, surge abscôndita nas minhas cogitações.

A internet convoca-nos para o *Admirável Mundo Novo,* de Aldous HUXLEY, o início da concretização de uma utopia [distópica?], um *local* onde encontramos uma panóplia fantástica das melhores coisas que a criatividade humana tem para oferecer. E o seu contrário, porquanto há na internet um conjunto infinito de páginas onde podemos descobrir todas as informações que desejamos e tantas outras que preferíamos não encontrar. Porque, se a rede mundial de computadores é uma grande cidade, com largas avenidas e jardins, com extasiantes monumentos por onde circulam deslumbrantes conteúdos, a internet também são becos escusos, ruas feias e sujas, proibidas ou

3 HOBBES, Thomas - *Leviatã*. Trad. João Paulo Monteiro/Maria Beatriz Nizza da Silva. 4ª Ed. Lisboa: Imprensa Nacional Casa da Moeda, 2010, p. 43.

desaconselhadas a crianças[4]. E a adultos. Porque na mesma rede onde circula o *belo*, podemos encontrar o mais repugnante da fealdade humana, não fosse a internet construída por mulheres e homens, com as suas imperfeições e contradições, não sendo perfeita, *porque o humano é imperfeito* e a internet um espelho da dimensão axiológica da condição humana.

Começar esta diáspora por recordar que a internet também é ignóbil, não é escamotear as suas inequívocas vantagens, até porque não consigo percecionar o futuro sem ela; faço-o, *in primis*, porque a rede que está subjacente a este estudo é a internet onde circula a pornografia e a pedopornografia, onde crianças são atraídas por predadores sexuais, onde os mais frágeis são vítimas de *bullying e* de discurso de ódio, onde se promove a anorexia, a bulimia e o suicídio, e os estupefacientes estão à distância de um simples *click*. Perigos reais, inflamados por uma imprensa, que esqueceu o seu *ethos*, desvaloriza o *logos* e está sôfrega pelo *pathos*, sempre ávida de alcoviteirices, transvestidas como notícias, fáceis de digerir por um consumidor pouco exigente, inapto para questionar, que aceita como dogmas todas as irrelevâncias que são jorradas pelos órgãos de comunicação (especialmente a televisão e a imprensa mais sensacionalista), que, historicamente, têm condenado a internet pela corrupção da inocência infanto-juvenil, o isolamento dos cidadãos, o crescimento do número de divórcios, criando alarde social para os relacionamentos virtuais, o *role playing*, e difundido fantasmas sexuais, dissociando estas situações, que sem dúvida sucedem no "mundo virtual", do devir social, da revolução de mentalidades que saiu do Maio de 68, da sociedade pós-cristianismo, do triunfo do consumismo, da sociedade do espetáculo e do império narcisista do hedonismo.

Como ensinou o poeta, *grande é a poesia, a bondade e as danças, mas o melhor do mundo são as crianças*, pelo que, nestas linhas, vou cingir-me a procurar responder a uma única e singela questão: *como proteger as crianças dos conteúdos nocivos disponíveis na internet?* Mas sem histeria: o desejo de tornar a rede mais amiga das crianças não nos pode motivar a "incendiar a casa apenas para assar o porco"[5]. Porque, de todos os riscos

4 Uso a expressão "criança" no seu sentido técnico-jurídico que decorre, *v.g.*, da Convenção sobre os Direitos da Criança; o que não significa que adira acriticamente ao mesmo: insistir em chamar criança a quem tem dezassete anos é abstruso.

5 AKDENIZ, Yaman - *Governance of Pornography and Child Pornography on the Global Internet: A Multi-Layered Approach*. *In*: EDWARDS, Lilian/WAELDE, Charlotte - *Law and the Internet. Regulating*

que a internet oferece às crianças, o maior perigo é o risco de as crianças serem excluídas da internet.

2. QUAIS OS CONTEÚDOS DISPONÍVEIS QUE MALTRATAM AS CRIANÇAS?

Dessarte, é preciso resistir a tentações quixotescas e distinguir os moinhos de vento dos verdadeiros perigos e riscos. Com efeito, demasiado condicionados pela influência tecnológica, os *ciberfóbicos* construíram um pessimismo difuso, que mereceu o carinho da imprensa mais sensacionalista, considerando a atual geração medíocre, que apenas se interessa por roupas, *Facebook*, carros, telemóveis, televisão, música *pop e rap*, e drogas. Uma geração mentalmente ágil mas néscia, culturalmente ignorante, que aprendeu milhares de coisas novas, mas, incapaz de interpretar um texto, recordar factos, compreender política externa, vazia de conhecimentos de história, religião e arte, inapta para escrever sem erros e viciada na cultura do *copy-paste*. Os pessimistas diabolizam os novos meios de comunicação, acusando-os de explorarem a vulnerabilidade das crianças, arrancando-as da sua ancestral pureza, destruindo a sua inocência, desumanizando-as, e enfeitiçando-as com a tecnologia, ao destruir as formas naturais de cultura e comunicação, e isolando os jovens da família e dos amigos, estimulando-lhes comportamentos antissociais, anunciando o colapso moral da infância e posteriormente de toda a humanidade. Uma geração que não tolera o silêncio (em sentido literal ou figurado), que prefere a companhia, real ou virtual, dos seus pares a um livro, monumento ou espetáculo, destituída de curiosidade intelectual, um "pequeno exército de narcisistas", (a geração "eu primeiro"[6]), que apenas quer aprender aquilo que é necessário para o seu sucesso imediato. Por todos, recordo VIRILIO, que se mostra francamente resistente às tecnologias, acusando-as de produzirem "drogados das redes multimídia, os *net-junkies*, os *webaholics* e outros *ciberpunks* acometidos pela doença IAD (*Internet Addiction Disorder*), cuja memória se torna um birquebraque"; [O A. não hesita em afirmar que, da utilização das novas tecnologias da informação,] "emergirá uma verdadeira crise no

Cyberspace. Oxford: Hart Publishing, 1997, p. 233; a expressão deverá ser atribuída a FRANKFURTER, no *Processo Butler v. Michigan*, conforme BOYLE, James - *Foucault in Cyberspace: Surveillance, Sovereignty, and Hard-Wires Censors*. "University of Cincinnati Law Review". Cincinnati. v. 66 (1997), p. 190.

6 BECK, Ulrich - *World Risk Society*. Cambridge: Polity, 2008, p. 9.

mundo, de consequências tão catastróficas como foram Auschwitz e Hiroshima"[7]. Se procurar resumir o pensamento apocalítico sobre a influência da tecnologia na infância, posso afirmar que "a nossa juventude adora o luxo, é mal-educada, despreza a autoridade e não tem o menor respeito pelos mais velhos. Os nossos filhos hoje são verdadeiros tiranos [...] respondem aos pais e são simplesmente maus"[8]. E estes assombros de pessimismo fazem temer que inexista uma contracultura que defenda as crianças.

É minha convicção que a frase de SÓCRATES foi tão exagerada há dois mil e quinhentos anos como seria hoje. Parece-me evidente que, se os menores aprendem as coisas de forma diferente dos seus pais ou dos seus avós, não significa que eles não as aprendam[9]. Pelo que, não vou apelidar a juventude coeva como "*the dumbest generation*"[10]; não apenas porque o adjetivo é acintoso, como, ainda que o mesmo se pudesse aplicar ao espaço cultural americano, seria absurdo importá-lo para uma realidade social como a portuguesa, a qual apenas recentemente abandonou uma ditadura que fez do analfabetismo/iliteracia um meio de controlo social.

Mas, se não sufrago as teorias catastróficas, não consigo subscrever que a "revolução tecnológica"[11] esteja a criar uma "geração mais aberta, mais democrática, mais criativa e com maior capacidade de inovação do que a geração anterior"[12], uma geração parida num mundo onde todos serão sapientes e irão adquirir mais facilmente autonomia psicológica.

---

7 VIRILIO, Paul - *A Bomba Informática*. Trad. Luciano Vieira Machado. São Paulo: Estação Liberdade, 1999, p. 43.
8 SÓCRATES (embora exista controvérsia sobre a autoria da frase, conforme TAPSCOTT, Don - *Grown Up Digital: How the Net Generation is Changing the World*. New York: McGraw Hill, 2009, p. 344). Ou, semelhantemente, "não tenho mais nenhuma esperança no futuro do nosso país se a juventude de hoje tomar o poder amanhã, porque esta juventude é insuportável, desenfreada, simplesmente horrível" (HESÍODO, 720 a.C.).
9 Assim, PALFREY, John/GASSER, Urs - B*orn Digital: Understanding the First Generation of Digital Natives*. New York: Basic Books, 2008, p. 241.
10 BAUERLEIN, Mark - *The Dumbest Generation. How The Digital Age Stupefies Young Americans and Jeopardizes Our Future (or Don`t Trust Anyone Under 30)*. New York: Penguin, 2008, *passim*.
11 CASTELLS, Manuel - *The Rise of the Network Society*. 2 Edition. Oxford: Blackwell Publishing, 2000, p. 1.
12 BUCKINGHAM, David - *Introducing Identity*. *In*: BUCKINGHAM, David - *Youth, Identity and Digital Media*. Cambridge, MA: The MIT Press, 2008, p. 13 [trad. nossa].

Humildemente, entendo que o erro na análise corresponde a desejar que a geração atual tenha os mesmos interesses que as gerações anteriores, sem compreender que o mundo e as crianças mudaram. Que há uma imensidão de estímulos que não existiam no passado. É insofismável que a geração atual lê menos (livros) que as anteriores, tem menores conhecimentos de história, geografia e filosofia, escreve com mais erros e toda uma panóplia de outros vícios e falhas que lhe são imputados: mas, também é verdade, as análises comparativas têm demonstrado que o QI está num crescimento ininterrupto desde o final da Segunda Grande Guerra[13]. Premissas só paradoxais na superfície, sendo paradigma de uma sociedade que exige conhecimentos mais práticos, aptidão para as competências profissionais, através de um ensino hipercompetitivo e seletivo, que exige resultados excecionais em áreas muito específicas, a *performatividade* a que alude LYOTARD[14].

Assusta que as novas gerações tenham perdido o prazer da leitura. E mais do que não ler, aterroriza o facto de que não apreciar literatura seja assumido com orgulho. Mas, presos a estereótipos, somos incapazes de questionar se será assim tão transcendentalmente importante ler livros: por mais que nos assuste, não existem hoje outros meios que permitam à criança receber os estímulos outrora oferecidos pelos livros? E, recordo S. Tomás de AQUINO, o qual "considerava que nem Sócrates nem Nosso Senhor puseram por escrito os seus pensamentos, porque a espécie de interação das mentes que é ensinar não é possível por meio da escrita"[15].

13 O argumento impressiona mas não é impressionante. Existem várias razões que podem explicar o crescimento do QI, como as melhores condições de vida, de nutrição, a entrada mais prematura para o sistema de ensino, *inter alia*. Sobre o tema, *vide* CARR, Nicholas - *The Shallows: What the Internet is Doing to Our Brains*. New York: W.W. Norton & Company, 2010, pp. 144 e ss.

14 Uso a expressão no sentido que perfilhei a LYOTARD, Jean-François - *A Condição Pós-Moderna*. 2ª Ed. Trad. José Bragança de Miranda. Lisboa: Gradiva, 1989, p. 98.

15 McLUHAN, Marshall - *A Galáxia de Gutenberg: a Formação do Homem Tipográfico*. Trad. Leônidas Carvalho e Anísio Teixeira. 2ª Ed. São Paulo: Editora Nacional, 1977, p. 47. A desvalorização da escrita também surge em TOFFLER, Alvin - *A Terceira Vaga*. Trad. Fernanda Pinto Rodrigues. Lisboa: Livros do Brasil, 1984, pp. 346/347.

A relação entre as crianças e o mundo da internet – como no passado entre as crianças e a televisão, ou mesmo a influência da música *rock*[16], ou da boneca *barbie*[17] – tem sido, nos últimos anos, objeto de discussão entre académicos dos mais heterogéneos ramos do saber e tema recorrente no debate público, numa contenda em que as premissas são apresentadas como contraditórias entre si numa dicotomia quase esquizofrénica; se fizer um esforço de simplificação – assumindo os perigos do minimalismo –, posso considerar que se digladiam duas correntes: os utópicos (ou *utopistas*[18]), que sustentam que a internet melhorou a qualidade da nossa vida social, enquanto os distópicos asseguram que a tecnologia está a corromper a juventude. Como, ambivalentes são as posições sobre as crianças e as tecnologias: com a mesma ênfase que desejamos que os nossos jovens cresçam *informatizados*, que dominem as novas técnicas e que através destas sejam hábeis na competitiva economia global, tememos os efeitos nefastos da sua exposição à tecnologia.

Não vou tomar posição sobre a querela; porque a tecnologia não é intrinsecamente boa nem intrinsecamente má! E, como bem reconhece um dos maiores entusiastas dos efeitos da internet nas novas gerações[19], a inclusão da tecnologia na vida das crianças é boa para algumas e péssima para outras! A tecnologia tem sempre uma biunivocidade na sua interação com as pessoas, e o inventor de uma arte nunca é a pessoa mais habilitada para dissertar sobre as suas valências, porque "uma coisa é inventar uma arte, outra julgar

16 Que era considerado emocionalmente agressivo, sendo um estímulo à masturbação [o autoabuso] e ao uso de drogas ilícitas (assim, ELKIND, referido por BUCKINGHAM, David - *Crecer en la Era de los Medios Electrónicos*. Trad. Roc Filella. Madrid: Ediciones Morata, 2002, p. 34 e TAPSCOTT, Don - Growing Up Digital: The Rise of the Net Generation. New York: McGraw Hill, 1998, p. 49. Semelhante visão, podia apreender-se nas revistas femininas portuguesas dos anos sessenta, onde se pode ler o seguinte trecho: "Deus nos defenda de que as nossas filhas enveredem por esse caminho de histeria coletiva. O *rock and rol* [...] deve ficar para além das fronteiras onde a dignidade, a pureza dos costumes e a integridade da mulher são um exemplo para o mundo" (conforme ABOIM, Sofia - *A Sexualidade dos Portugueses*. Lisboa: FMMS, 2013, p. 61).

17 Os perigos da *Barbie*, como um símbolo do novo feminino que irradia liberdade, prazer consumista e sexo, que vai introduzir as crianças prematuramente na adolescência e esterilizar modos de vida era enfatizado por ALLEN, David - *Is Childhood Disappearing?* [Em linha]. Brighton: University of Sussex. [Consult. 13 mar. 2013]. Disponível em: http://www.sussex.ac.uk/cspt/1-6-1-2-6.html<, p. 16.
Sobre a sexualização da boneca *Barbi*e, *vide* MAINE, Margo - *Something's Happening Here: Sexual Objectification, Body Image Distress, and Eating Disorders*. In: OLFMAN, Sharna - *The Sexualization of Childhood*. Connecticut: Praeger, 2009, p. 68. Sobre a sexualização das bonecas, em geral, *vide* BAUDRILLARD, Jean - *A Sociedade do Consumo*. Trad. Artur Morão. Lisboa: Edições 70, 1975, pp. 251 e ss.

18 No sentido oferecido por CUNHA, Paulo Ferreira da - Geografia Constitucional: Sistemas Juspolíticos e Globalização. Lisboa: Quid Juris, 2009, p. 25.

19 TAPSCOTT, Don - *Growing Up Digital*, *cit*., passim.

os benefícios ou prejuízos que dela advirão para os outros"[20]. E, se a internet tem inegáveis vantagens para o desenvolvimento das crianças, são inegáveis os perigos para o processo formativo da criança. Até porque, se é absolutamente notável a bonomia com que as crianças lidam com a tecnologia, se é fácil espantarmo-nos quando uma criança de dois anos domina a linguagem de um *tablet* ou quando, aos quatro, ensina os avós a usar um telemóvel, também é notável que uma criança desta idade seja fluída numa língua complexa como o mandarim. Mas, importa recordar, o mundo está cheio de metáforas moribundas e não perder a perspetiva: se uma criança nasceu e cresceu na China, é normal que domine esta língua.

De outro ponto de vista, é preciso a humildade de reconhecer que nos faltam respostas para pugnar por certezas absolutas. Por exemplo, pergunta-se: os jovens recordam a informação que consomem na internet melhor ou pior do que a que consomem em material impresso?[21] São efetivamente capazes de realizar cumulativamente várias atividades ou a capacidade de multitarefas é um mito?

Algum niilismo que *transpirou* destas cogitações está umbilicalmente relacionado com o objeto deste estudo. Porque a internet sobre a qual reflito não é aquela por onde navega *o belo, o bem e o justo*. A rede em que mergulhei é, desde logo, a *DeepWeb*, lugar obscuro onde encontramos o mais abjeto da criatividade humana, uma rede (privada?) na qual se partilham conteúdos ilícitos, numa ilegalidade que pode consubstanciar-se em algo moralmente (quase) inócuo, como a violação dos direitos de autor ou algo tão vil como a pedopornografia[22], lutas até à morte, imagens de violações, fóruns jihadistas, fraudes bancárias, onde é possível comprar drogas, armas, órgãos, animais em vias de extinção (que confortavelmente nos são entregues em casa, através de legítimas empresas

20 PLATÃO - *Fedro ou da Beleza*. Trad. Pinharanda Gomes. 6ª Ed. Lisboa: Guimarães Editores, 2000, p. 121.
Pensemos em Johannes GUTENBERG, o pai da imprensa, cristão convicto, que, ao publicar a Bíblia para espalhar a palavra do Senhor, tornou-se no maior inimigo da Igreja, porquanto, foi graças ao seu trabalho que foi possível colocar uma Bíblia em cada casa e se estabeleceu a arquitetura que permitiu a LUTERO iniciar a Reforma (como eu, POSTMAN, Neil - *Technopoly: The Surrender of Culture to Technology*. New York: Vintage Books, 1993, p. 15).
21 A questão é formulada por PALFREY, John/GASSER, Urs - *Born Digital: Understanding the First Generation..., cit.*, p. 239.
22 Hoje já não é verdadeira a frase de JENKINS que enfatizava como era simples encontrar conteúdos pedófilos na rede (JENKINS, Philip - *Beyond Tolerance: Child Pornography on the Internet*. New York: New York University Press, 2001, p. 3).

de transporte de encomendas, porquanto, o produto ilícito, vem dissimulado em livros ou algo semelhante), escravos sexuais (em regra, crianças, que aqui têm um colossal valor comercial), e qualquer outro "bem" que a perversidade humana seja capaz de tentar adquirir. A *DeepWeb* é um mundo secreto [ainda que cada vez menos] dentro do mundo da internet, uma fronteira desconhecida para a maioria dos utilizadores, onde é possível encontrar o mais tenebroso que a crueldade humana tem para oferecer, que recebeu atenção mediática quando o cidadão alemão Armin MEIWES (que atingiu a *imortalidade* com o cognome de "Canibal de Rotenburg"), colocou um anúncio pessoal, num fórum dedicado ao canibalismo, em que dizia: "procuro homem bem constituído, 18-30 anos, para ser esquartejado e consumido"[23].

A internet sobre a qual se debruça este texto é [também] a internet da Megan MEIER. Megan foi uma cidadã americana, nascida na cidade de Dardenne Prairie, Missouri, que teve uma desavença com duas amigas, por, alegadamente, ter feito comentários desagradáveis sobre elas. Estas, em conluio com os seus pais, criaram um perfil falso de um rapaz – Josh Evans – que demonstrou um interesse sentimental e erótico em Megan e com quem esta, posteriormente, começou a partilhar (in)confidências. Megan apaixonou-se por este "rapaz" e, quando descobriu o logro, cometeu suicídio por enforcamento, um mês antes de completar os catorze anos. Presumivelmente, o esquema teria sido montado para conseguir obter informações e conteúdos de Megan, que tornassem possível humilhá-la. Haley MACKLIN era uma aluna notável mas que ambicionava popularidade. Para a alcançar, tornou-se amiga de um grupo de colegas; movidas, alegadamente, por um móbil semelhante, seis adolescentes atraíram-na a casa de uma delas e, durante mais de trinta minutos, agrediram-na brutalmente, deixando-a inconsciente e com lesões permanentes; as imagens da agressão foram gravadas para posterior disponibilização na rede (e ainda estão disponíveis na rede; mas, pelas razões

23 E, estranhamente, Bernd Jürgen BRANDES respondeu: "ofereço-me a ti e deixar-te-ei jantar o meu corpo vivo". A indignidade da história exige que a mesma seja proscrita do corpo do texto e que surja "dissimulada" numa nota de rodapé, porquanto, em março de 2001, MEIWES e BRANDES relacionam-se sexualmente; depois, MEIWES rezou pelo companheiro e planearam juntos como aquele seria devorado por este. De acordo com o planeado, MEIWES amputou o pénis de BRANDES, para depois ambos o comerem, após o fritarem, temperado com pimenta e alho (alegadamente BRANDES não chegou a comer, porque achou a carne demasiado dura). Após a morte de BRANDES, Armin comeu cerca de 20 kg do seu corpo, tendo assegurado em entrevista que o sabor da carne era "semelhante ao da carne de porco, um pouco mais amarga e mais forte, mas um sabor muito bom". Todo este ritual ficou documentado em vídeo, de forma a poder ser partilhado na *DeepWeb* (os sórdidos pormenores do caso podem ser consultados, *v.g.*, aqui: http://pt.wikipedia.org/wiki/Armin_Meiwes< [Consult. 14 fev. 2013].

supra invocadas, não deixo no texto uma ligação eletrónica para as mesmas)[24]. Semelhantemente, Hannah SMITH, uma jovem britânica de catorze anos, uma entre 60 milhões de utilizadores (metade destes menores), que aderiu à rede social *ask.fm* com sede na Letónia. No seu perfil, colocou uma foto (absolutamente normal) que, por inescrutáveis razões, foi mal recebida na comunidade. Reiteradamente, a jovem foi vítima de insultos, sendo que, entre estes, foi recorrente a alusão para que se matasse. A jovem procurou ignorar o assédio e, não o conseguindo, contactou a rede social para que a mesma tomasse medidas. Segundo a imprensa, a empresa estava a analisar a queixa. Uso o verbo no pretérito, porque Hannah enforcou-se no seu quarto, no dia 2 de Agosto de 2009. Muitos anos antes de as *baleias serem alegadamente azuis*...

Uma (outra) situação, profusamente mediatizada, foi o caso *Cathedral*, que ocorreu, em 1996, na Califórnia: uma menina de dez anos foi passar o fim de semana a casa de uma colega de escola; o pai desta trancou a criança no seu quarto, onde tinha um computador com acesso à internet, tendo, não apenas abusado da menina, como filmado e divulgado a agressão sexual. Porque a divulgação ocorreu em tempo real, aceitou instruções de quem assistia ao "espetáculo", satisfazendo as sugestões que lhe eram propostas pelos ogres. Igualmente com grande cobertura da imprensa, a operação *KOVA*, em 2005, na qual a polícia espanhola prendeu cinco pessoas que, fazendo-se passar por uma empresa de *baby-sitters*, abusavam sexualmente de crianças (algumas com idade inferior a um ano), quando os pais se ausentavam de casa e os deixavam a cuidar dos seus filhos; também neste caso, as imagens dos abusos foram divulgadas na internet.

Uma prática recorrente no mundo telemático consiste em convencer adolescentes de que se trabalha no mundo da moda, televisão ou cinema, para angariar fotografias ousadas; ofereço o exemplo de Joshua THERELKELD, que se fazia passar por uma agente de modelos e, deste modo, iludir raparigas e convencê-las a enviar fotografias desnudas. Joshua, de 32 anos, criou um perfil falso no *MySpace* com o nome de Sara Miller e ludibriou cerca de cem jovens, obtendo delas fotografias eróticas, que, posteriormente, vendia a uma empresa de pornografia. Joshua foi desmascarado após a mãe de uma adolescente ter acionado a polícia, ao descobrir que a filha se havia

24 A história de Haley foi retratada no filme *Girl Fight*, dirigido por Stephen GYLLENHAAL.

encontrado pessoalmente com o maníaco, na cidade de Orange County, onde posou para fotografias e manteve relações sexuais.

Chris STANOFORTH, de 20 anos, morreu numa ambulância a caminho do hospital local, na cidade inglesa de Sheffield. Segundo o seu pai, o jovem estava havia dez horas, a jogar na sua consola. Como fizera inúmeras outras vezes, porque vivia para este jogo (o jogo em causa era o *Halo*). De acordo com os médicos, o jovem faleceu devido a uma trombose originada por vários períodos de atividade sedentária. A morte de Chris foi semelhante a outras ocorridas em países asiáticos, o que obriga o intérprete a questionar-se sobre o poder aditivo dos jogos virtuais. Sendo que não seria preciso morrer ninguém, para que a pergunta se exigisse. Como, não são precisos estudos científicos para exprimir uma evidência: os *nativos digitais*[25] passam demasiado tempo agarrados aos computadores, com consequências para a sua saúde que importa dissecar, para compreender.

Dito isto, não embarco em demagogias e, *ab initio*, deixo claro que os casos trágicos que ofereci são exceções, exacerbados como parte de uma narrativa que tem pautado as últimas décadas, um lastro de *internetfobia* que circula pelos *media*, com a enfatização (efabulação) e hipervalorização dos riscos – que existem, que são reais e perigosos –, e que formou a *tempestade perfeita* para uma intervenção castradora dos Estados, alicerçada no pânico provocado nos pais. O número de crianças que faleceu em consequência de atos relacionados com a internet é residual, sendo uma insignificância estatística. Os estudos recentes comprovam[26] que a vitimação *online* é uma das menos comuns ameaças às crianças, e que existe um oceano que separa a realidade e a propaganda emanada pelos órgãos de comunicação social. Afirmo-o, convicto que, para a maioria dos menores, a internet é uma experiência segura e positiva. Até porque, os exemplos que deixei escritos, que são cruéis, que nos enojam, nada revelam sobre a

25 PRENSKY, Marc - Digital Natives, Digital Immigrants. From On the Horizon. [Em linha]. [s.l.]: Marc Prensky. [Cons. 19 Fev. 2011]. Disponível em: http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf<,

26 Conforme MITCHELL, Kimberly J. [*et al*.] - *Youth Internet Victimization in a Broader Victimization Context*. "Journal of Adolescent Health". New York. v. 48, Iss. 2 (February 2011), p. 130.

internet. Estes casos têm por objeto a brutalidade da condição humana: a internet é meramente acessória, pelo que, não podemos tomar a nuvem por *Juno*.

Se a internet está contaminada por riscos, importa não dramatizar: a maioria dos perigos que arrepia os pais e a sociedade civil são realidades que existem há décadas (se não há séculos), e que podem ser vivenciadas por quem não tem internet. Como, se reconheço que navegam pela internet navios carregados de perigos para as crianças, não as podemos fechar na caverna de PLATÃO e privá-las das novas tecnologias. Nem por um instante duvido da imensa importância que a rede tem para o desenvolvimento dos jovens e considero que o acesso aos novos meios da sociedade da informação é um direito fundamental de quarta geração, que não lhes pode ser sonegado.

Acresce que, o facto de os mais jovens serem as mais frágeis das vítimas da internet não pode causar estupefação. Porque, também fora da internet, os jovens são vítimas privilegiadas: as crianças são duas ou três vezes mais suscetíveis que os adultos de serem vítimas de roubos, violações, agressões físicas graves e toda uma panóplia de crimes violentos.

Não obstante, tem sido recorrente uma (mega/meta-)narrativa sobre os riscos da internet, sobre os quais abundam opiniões, mas faltam pesquisas, mais baseadas em argumentos emotivos do que racionais, pelo que a perigosidade da internet é uma realidade por todos aceite, sem que seja questionada.

Porque entendo ser crucial a compreensão (e também a desconstrução) desta narrativa, proponho-me realizar uma abordagem tópica sobre os riscos mais prementes a que as crianças são expostas na rede, tendo como cardápio as mais recorrentes ameaças que maltratam as crianças, procurando discernir entre a realidade e a ficção, entre os perigos e os mitos.

Começo a minha diáspora por trazer à colação uma realidade que tem suscitado o interesse dos investigadores e o pânico dos pais: a problemática da exposição das crianças à pornografia. Como regular a rede de modo a proteger as crianças de conteúdos pornográficos gerou um verdadeiro pânico moral, uma "narrativa histérica"[27] que contagiou a imprensa, a sociedade civil, os líderes religiosos, os juristas e os Estados. E, por (algumas) razões intuitivas, é insofismável que a internet veio facilitar o acesso à pornografia; não apenas estes conteúdos estão disponíveis em muito maior quantidade e variedade, como a rede permite ao consumidor ultrapassar o constrangimento e derrotar as inibições que o dominavam ao (tentar) adquirir revistas ou filmes com teor pornográfico ou em entrar numa sala de cinema da especialidade. No resguardo do lar, hoje, é, extremamente, fácil ter acesso a uma imensa e variada panóplia de conteúdos pornográficos. Sendo que, este consumo, é realizado por adultos e, também, por crianças. Quer deliberada, quer inadvertidamente. E de um modo difícil de controlar, porquanto na internet, *ninguém sabe se és um cão* ou uma criança. Adicionalmente, fenómenos como o *sexting* contribuem para exacerbar o pânico moral sobre as consequências, para o desenvolvimento psicossocial e sexual das crianças, decorrentes de um acesso fácil à pornografia.

O receio que estes comportamentos provocam torna compreensível o pensamento daqueles que sustentam a proscrição dos conteúdos pornográficos da internet ou a exigência de medidas para impossibilitar que os menores tenham acesso aos mesmos. Se aceitarmos o argumento, e pretendermos embarcar numa cruzada contra a pornografia, surge uma questão prévia que lhe é prejudicial: o que é pornografia?[28]

As definições selecionam e refletem uma realidade, mas não raramente desfiguram-na, porque a realidade é sempre mais rica e complexa e, com subtilezas que não se conseguem desenhar nas definições; mas estas são quadros mentais imprescindíveis que nos permitem *beber* a realidade. No caso da pornografia, não obstante a dificuldade,

27 SHOWALTER, Elaine - *On Hysterical Narrative*. "Narrative". Ohio. v.1, n.1 (1993), pp. 24 e ss.
28 As minhas dúvidas também são as de DIAS, Jorge Figueiredo - *Anotação ao artigo 171º. In*: DIAS, Jorge de Figueiredo [Dir.] - *Comentário Conimbricense do Código Penal*. Coimbra: Coimbra Editora, 2012, p. 837.

"definir *oblige",* porquanto, não se trata de averiguar *se a neve é efetivamente branca*[29], mas procurar capturar esta realidade complexa. Perscrutando na linguística, esta surge definida como *colecção de pinturas ou gravuras obscenas; característica que fere o pudor (numa publicação, num filme, etc.); obscenidade, indecência, licenciosidade; qualquer coisa feita com o intuito de ser pornográfico, de explorar o sexo tratado de maneira obscena*, sendo pornográfico o *que demonstra, descreve ou evoca luxúria ou libidinagem; indecente, imoral, libertino*[30]. A profícua compreensão do conceito obriga a cotejar o significado de erotismo, palavra de origem grega (*erotikós*), que deriva do Deus grego do amor EROS, e que *apela ao amor, paixão, desejo intenso, plasmando-se numa manifestação explícita de sexualidade*, porquanto, segundo as regras da lógica, as definições também se constroem pelo estabelecimento das diferenças e, quando procuramos a destrinça, revela que a pornografia apela diretamente à excitação sexual, enquanto que o erotismo é interpretado como uma manifestação artística (o que, em rigor, remete a diferenciação para os juízos estéticos).

Procurando densificar, por pornografia entendo a exposição explícita dos órgãos sexuais, da zona púbica ou de um ato sexual de relevo, tendo como finalidade provocar excitação sexual no observador. A pornografia é íntima da obscenidade, o que fere o pudor, o que, pela sua inconveniência, não está de acordo com as regras de decoro, sendo, inequivocamente, uma construção social, datada e situada; se o ato sexual na intimidade da privacidade não é obsceno, a sua exibição pública será considerada indecente. A pornografia é uma narrativa, através de imagens, sons ou palavras, da sexualidade, que se carateriza por tornar público o que, de acordo com o sentimento da comunidade, deveria ser privado, tendo como desiderato provocar excitação sexual. A intenção é determinante para distinguir a pornografia, *v.g.*, da exibição dos órgãos sexuais com fins educativos ou científicos (uma aula de anatomia), com finalidades artísticas (uma pintura, um filme, *etc*.). Mas, não isenta de dificuldades: posso afirmar que um filme será erótico, logo, não pornográfico, quando a reprodução de órgãos sexuais ou de um ato sexual, apesar de suscetível de provocar excitação sexual, obedece a um qualquer efeito estético ou

29 Referimo-nos à discussão filosófica abordada, *v.g*., em MALATO, Maria Luísa/CUNHA, Paulo Ferreira da - *Manual de Retórica & Direito*. Lisboa: Quid Juris, 2007, p. 61.
30 Dicionário Houaiss da Língua Portuguesa.

pretende transmitir uma qualquer ideia ou mensagem. O que é uma noção profundamente subjetiva, que fica pendente de perceções de sensibilidade individuais.

Pessoalmente, considero que a melhor definição de pornografia foi a oferecida por Potter STEWART[31], quando afirmou que não sabe explicar o que é mas que, quando a vê, reconhece-a! (o que me convoca as palavras de Santo AGOSTINHO, quando questionado sobre como se define o tempo: *se ninguém me perguntar, eu sei, se desejar explicá-lo àquele que me perguntou, não sei*).

A narrativa moral dos perigos do acesso a conteúdos sexuais pelas crianças é íntima da conceção da criança como ser inocente e assexuado, do desejo dos pais de manterem os seus filhos (e, especialmente, as filhas, *in casu*, *o direito dos pais à virgindade das filhas*) imaculados pelo maior tempo possível[32] [a expressão *perder a virgindade* é sintomática de uma sociedade que, apesar da alegada libertação dos costumes, ainda interpreta a virgindade (feminina!) como um valor moral a preservar]), porquanto, o conceito de que *naturalia non sunt turpia* não está inscrito no ADN de uma sociedade que ainda não derrotou os preconceitos vitorianos, continuando propensa a uma política antilíbido que não aceita que o amor possa ser mais destrutivo que o sexo.

É irrefutável que a sexualidade é um elemento central da vida dos adolescentes como, nem os mais distraídos ignoram, que, contrariamente a Valter Hugo MÃE, que só *não [lhe tocou] ainda, porque me seduz a proximidade da primavera e a ideia de esperar*[33], os adolescentes iniciam-se sexualmente cada vez mais cedo. E que o fazem com uma desinibição que assusta os adultos.

31 Refiro-me a uma citação no Processo *Jacobellis v. Ohio* 378 U.S. 184 (1964).
32 "A atenção do Estado para estas questões não representa uma inovação, pois um estudo atento da história do *mass media* neste século levar-nos-ia a constatar que o debate sobre conteúdos ofensivos acompanhou as indústrias de massa em torno da pintura, os livros, as gravações áudio, filmes e mais tarde o vídeo, videotexto e a televisão *pay-per-view*. Levando-nos a concluir, que muitas inovações nas tecnologias de informação e comunicação são experimentadas e desenvolvidas pela indústria de conteúdos para adultos" (CARDOSO, Gustavo - *As Causas das Questões ou o Estado à Beira da Sociedade de Informação*. "Sociologia, Problemas e Práticas". Lisboa: CIES-ISCTE/CELTA, p. 122).
33 MÃE, Valter Hugo - *pornografia erudita: a virgindade da madalena*.

Mas, importa recordar, não é apenas na internet que sexo, erotismo e pornografia abandonaram o *bas-fond* para invadir o *mainstream* e adquiriram uma inaudita centralidade num tempo pansexual: e, reiteradamente, os pais que mais se indignam com o acesso dos seus filhos a estes conteúdos são os mesmos que espalham, despreocupadamente, pela casa, revistas com elevado cariz erótico ou os que consomem estes conteúdos em família, através dos programas de televisão.

Devassando seara alheia, assumo o risco de afirmar que expor crianças a conteúdos pornográficos poderá ser nefasto para o seu desenvolvimento psicossexual e suscetível de lhes transmitir uma noção transviada da sexualidade, que fomente nos jovens a construção da sua sexualidade tendo como paradigma o que consomem na internet[34], construindo uma geração que confunde o sexo com a pornografia.

No entanto, e ainda que ciente dos perigos (quiçá por androcentrismo), acredito que a proteção das crianças, que se deseja, que se exige, não se pode construir pela proibição incondicional dos conteúdos pornográficos na internet: dessarte, não podemos reduzir a oferta na rede, tendo como barómetro as crianças, banindo da internet todos os conteúdos que não são adequados para os menores: a internet não pode ter como padrão as crianças; numa feliz analogia, não "se pode transformar num "parque infantil""[35] e "os adultos serem tratados como crianças"[36].

Adicionalmente, importa sublinhar, a pornografia não se pode confundir com "iconografia sexual infantil": crianças que procuram *sites* de pornografia entre adultos é, diametralmente, diferente de adultos que procuram *sites* de pornografia com crianças. Têm natureza e perigos diferentes e não podem ser abordados como se da mesma

34 Neste sentido, ofereço as palavras das crianças: "a pornografia era as nossas aulas de educação sexual. Tudo o que víamos era o que absorvíamos como referência" (as palavras são de "Inês" e constam de uma reportagem sobre a sexualidade entre os 12 e os 16 anos, Revista Única, 22/10/2011, p. 52).
35 JOHNSON, Dawn L. - *It´s 1996: Do You Know Where Your Cyberkids Are? Captive Audiences and Content Regulation on the Internet*. "Journal of Computer & Information Law". Chicago, p. 97. Semelhantemente, MACHADO, Jónatas E. M. - *Liberdade de Expressão: Dimensões Constitucionais da Esfera Pública no Sistema Social*. Coimbra: Coimbra Editora, 2002, p. 1109.
36 AKDENIZ, Yaman - *Cyber-Rights & Cyber-Liberties (UK) Report - 'Who Watches the Watchmen: Internet Content Rating Systems, and Privatised Censorship'*. [Em linha]. Leeds: University of Leeds. [Consult. 10 Dez. 2013]. Disponível em: http://www.cyber-rights.org/watchmen.htm< [trad. nossa].

realidade se tratasse. Com a mesma veemência que tolero os primeiros, sou intransigente na perseguição dos segundos.

Sucede que, a complexidade da fenomenologia da iconografia sexual de crianças começa logo quando procuramos defini-la. Se, como vimos, definir pornografia é uma missão titânica, a demanda por uma definição de "pornografia infantil" é ainda mais intrincada, sendo que, o axioma *eu sei o que é quando a vejo*, não pode exportar-se para a definição de pedopornografia, porque esta pode existir, mesmo quando a maioria de nós não a consegue ver!

Numa aceção apriorística, posso afirmar que "pornografia infantil" é "toda a representação, por qualquer meio, de uma criança no desempenho de actividades sexuais reais ou simuladas, ou qualquer representação dos órgãos sexuais de uma criança para fins predominantemente sexuais"[37]. Mas, se a definição ajuda, não resolve. Começo por esclarecer que a pedopornografia não é uma qualquer foto de uma criança despida. A típica foto de um bebé no banho, ainda que desnudo, ainda que o órgão sexual esteja visível, não pode ser considerada, *tout court*, uma foto pedopornográfica; se um dos pais decidir publicá-la, *v.g.*, numa rede social, não poderá ser qualificado como um pornógrafo que dissemina pedopornografia na internet. O que não significa que a prática seja salutar. Permita-se-me que seja incisivo nos vernáculos a benefício da transmissão da mensagem: para um pedófilo, esta fotografia, mais do que erótica, é sexualmente excitante e masturbar-se-á a olhar a foto e ejaculará sobre a mesma. Pelo que, para colmatar a *sensibilidade e bom senso* dos parentes que disponibilizam estas fotografias na internet, nada deverá obstar a que um prestador de serviço em rede proíba contratualmente a sua disseminação, retirando-as dos seus servidores e apagando as contas de quem as disponibilize.

37 Protocolo Facultativo à Convenção sobre os Direitos da Criança relativo à Venda de Crianças, Prostituição e Pornografia Infantis.

Dessarte, perseguir a pedopornografia não pode ser entendido como uma forma de punir desejos e fantasias ou como uma limitação ilegítima à liberdade de expressão[38]. Sonhar e desejar ter *sexo* com crianças é penalmente inócuo. Consumir estes conteúdos não. Porque uma foto pedopornográfica é a prova do abuso sexual de uma criança e uma forma de o documentar. E, quando colocada na internet, fica na rede para sempre, sendo uma memória omnipresente e eterna de que aquela criança foi abusada. Ao que acresce o medo, ubíquo, de que a qualquer momento, qualquer pessoa possa ver as imagens do momento mais traumático da sua vida.

Sendo óbvio do ponto de vista analítico que a pedofilia não é uma doença do século XX, é indubitável que a internet provocou uma explosão de pedopornografia como em nenhum outro tempo histórico. Não nos iludamos e sejamos inequívocos em assumi-lo: a internet é um paraíso para os pedófilos, uma verdadeira repristinação da *cova do Caco;* se não tornou a pedopornografia legal, tornou estes materiais extraordinariamente acessíveis, com uma muito maior rapidez de propagação e (num primeiro momento) suscetíveis de serem consumidos (quase) sem risco. Os pedófilos deslocaram-se dos jardins e das proximidades das escolas para o resguardo de um computador e o "mundo virtual" permite-lhes uma aproximação das vítimas que, antes, só era possível quando escolhiam profissões ou *hobbies* que lhes consentiam uma proximidade discreta e tranquila com as crianças (como empregos nas escolas ou atividades ligadas à catequese, aos escuteiros, às prática desportivas) ou, ainda, quando se aproximavam de mães solteiras para ter acesso facilitado aos seus filhos.

Hoje, a internet – ou a forma descuidada como se utiliza a internet – possibilita que as redes sociais telemáticas funcionem como um cardápio para pedófilos e "predadores sexuais", oferecendo-lhes novos meios e novas oportunidades para monitorizar, angariar e atrair as suas "presas", bem como, usar a informação que, desleixadamente, está disponível, para se aproximarem das crianças e interagir com elas. Por outro lado, o agressor tem uma maior facilidade em esconder a sua identidade, pode metamorfosear-se como pretender, iludir as suas vítimas com falsas representações, usar meios decetivos

38 Mais assertivo que Catharine MaCKINNON será impossível: quando os homens se masturbam com estas imagens não "são ideias o que eles ejaculam" (MaCKINNON, Catharine - *Only Words*. Third Printing. Massachusetts: Harvard University Press, 1996, p. 17).

para aliciar menores, e, reiteradamente, assumir a identidade de uma criança ou adolescente para, desta forma, conseguir seduzir. Como, a *www* permite ao agressor sexual marcar encontros pessoais ou escondido na rede, ter conversas de cariz obsceno ou pornográfico, e, ainda, obter das suas vítimas imagens com o mesmo cariz. Como, a internet é hoje uma (a) porta de entrada para o turismo sexual e tráfico internacional de crianças, prostituição e pornografia infantis. Por fim, a internet é a pedra angular do surgimento de uma cultura de pedofilia, tendo oferecido os meios para o surgimento de uma comunidade de pedófilos, que deixaram de estar isolados e desenvolveram uma forte dinâmica de grupo e um *sentimento de pertença*, que lhes permite conversar, permutar experiências, fantasias, conteúdos, procurar a exculpação dos seus atos, instruir os mais novos sobre como devem atuar para se protegerem, permitindo-lhes sentar-se, noite após noite, para debater, em conjunto, a sua perversa paixão comum sem se sentirem marginalizados.

Todavia, se não oblitero a existência de pedofilia na rede, também não posso obliterar que alguns medos são exagerados e subscrevem o mito de que o universo internet é uma perigosa selva onde se colhe impunemente a pureza sexual dos mais débeis. Efetivamente, se não espanta que a pedofilia na internet seja a principal preocupação dos pais, da sociedade civil e dos Estados, esta é uma preocupação claramente exacerbada, construída mais sobre sensações e posições morais do que num debate racional. Até porque, numa época de profunda liberdade sexual, onde todas as práticas são permitidas e sugeridas pelos arautos da modernidade, por vezes ensinadas nos divãs dos terapeutas, onde se esbateram as fronteiras que separam o normal do perverso, em que tudo é lícito, desde que conduza à sagrada busca da felicidade individual, apenas a pedofilia continua consensualmente a ser considerada como uma perversidade que urge combater. E, mesmo esta (aparente) unanimidade na crítica, como bem sublinha com deliciosa ironia SIGUSCH, apenas é possível porque condenar a pedofilia "nada exige de nós senão o óleo de humanismo que tão efetivamente lubrificou no passado, as rodas da violência. Só alguns, contudo, se colocam seriamente a favor de programas capazes de salvar as vidas das crianças, já que custariam dinheiro e conforto ao mesmo tempo em que exigiriam a adopção de um modo de existência diferente"[39].

39 *Apud* BAUMAN, Zygmunt - *Amor Líquido: sobre a Fragilidade dos Laços Humanos*. Trad. Carlos Alberto Medeiros. Rio de Janeiro: Jorge Zahar Ed., 2004, p. 36.

Como James KINCAID chamou à minha atenção, achamos repulsiva a pedofilia, mas a nossa cultura está repleta de imagens pedófilas. Achamos repugnante e incompreensível que um adulto tenha interesse sexual por crianças, mas vivemos numa sociedade que erotiza a infância, em que aos 14 anos pode desfilar-se nas *passerelles* e ser eleita a *Super Model of the World*, em que enfatizamos como ideal de beleza o rosto e a pele suave, o corpo esguio (que tornou impossível perceber sensualidade nas mulheres de BOTTICELLI), idealizamos como lábios perfeitos os típicos de quem tem 14 anos, a boca de quem tem 11, adotamos uma depilação que nos remete para a pré-puberdade, elegemos a inocência e a pureza como valores erógenos, o "*baby talk*" desempenha uma função erótica e, depois, hipocritamente, ficamos indignados quando homens e mulheres desejam sexualmente crianças[40].

Quando convoco a problemática da erotização do mundo infantil e juvenil, não estou a sufragar a ignóbil narrativa pedófila, nem a contribuir para branquear o abominável, apenas a trazer à colação a necessidade de deixar amadurecer a infância das crianças e defender a liberdade sexual negativa dos pré-adolescentes.

Por outro lado, é importante desmistificar a crença popular de que abuso sexual de menores é sinónimo de pedofilia: "a maioria dos abusos não é praticada por indivíduos com o desvio de orientação sexual ou a parafilia que é designada por pedofilia"[41]; a maior parte dos abusadores não padecem de qualquer psicopatologia relevante, são cidadãos – e cidadãs – que em dado contexto da sua vida têm desejo erótico por uma criança ou é uma criança que está acessível ao abusador (o agressor regressivo ou situacional). E, porque nem todos os abusadores de crianças são pedófilos, é preferível a expressão "abusador sexual de crianças"[42]; "separar abusadores em "pedófilos" e "não pedófilos",

40 Assim, KINCAID, James R. - Erotic Innocence: The Culture of Child Molesting. Durham: Duke University Press, 1998, p. 17, que traz à colação estudos que me serviram de premissas. O A. constata que muitos adultos na nossa cultura têm, com base nestas, algum tipo de atração sexual por crianças (*Ibidem*, p. 25).

41 MANITA, Celina - *Quando as Portas do Medo se Abrem…: do Impacto Psicológico ao(s) Testemunho(s) de Crianças Vítimas de Abuso Sexual*. In: SOTTOMAYOR, Maria Clara - *Cuidar da Justiça de Crianças e Jovens: a Função dos Juízes Sociais: Actas do Encontro*. Coimbra: Livraria Almedina, 2003, pp. 231/232.

42 GOMES, Francisco Allen/COELHO, Tereza - *A Sexualidade Traída: Abuso Sexual Infantil e Pedofilia*. Porto: Ambar, 2003, p. 17.

em determinadas situações, pode parecer um preciosismo; [mas] tem vantagens, para compreender o fenómeno e preveni-lo, para o tratamento […] e para o prognóstico"[43].

A pedofilia consiste num desvio comportamental, num "interesse sexual prolongado por crianças com o desenvolvimento e maturidade física de um menor de 11 anos"[44], pelo que, os "pedófilos vêem os instintos sexuais estimulados pelas características físicas e psíquicas tipicamente infantis, que afastam o desejo sexual na esmagadora maioria dos adultos"[45]. Por seu turno, "um abusador sexual infantil não pedófilo não tem uma preferência erótica específica por crianças. O abuso da criança ocorreu por substituição, ou por se tratar de um ambiente infantil perturbado ou por ele próprio estar perturbado. A agressão sexual aconteceu, e foi sobre uma criança; mas, eventualmente, poderia não ter sido uma criança"[46].

Pelo que, as referências aos "predadores" *online*, que se aproveitam da ingenuidade das crianças e que usam truques e violência são, em grande parte, imprecisas; contrariamente ao estigma social criado e desenvolvido pelos *media*, estes predadores sexuais, em regra, não são pedófilos. Por inúmeras razões, os pedófilos têm dificuldade em angariar crianças na rede (para encontros pessoais); as crianças são menos acessíveis que os adolescentes, não apenas para entabular uma conversação, como para ter conversas de conteúdos pornográficos, como é, muitíssimo, mais complexo agendar um encontro pessoal com uma criança do que com um adolescente.

Estou ciente de que o que deixei escrito contraria *verdades construídas com bases em mitos urbanos* e narrativas desenvolvidas pela imprensa, tendo por base casos

43 GOMES, Francisco Allen/COELHO, Tereza - *A Sexualidade Traída..., cit.*, pp. 22/23.
44 HOWIT, *apud* LEITE, Inês Ferreira - *Pedofilia. Repercussões das Novas Formas de Criminalidade na Teoria Geral da Infração*. Coimbra: Livraria Almedina, 2004, p. 13. Assim, importa ter presente quais os critérios para o diagnóstico de pedofilia: 1. Ao longo de um período mínimo de 6 meses, fantasias sexualmente excitantes recorrentes e intensas, impulsos sexuais ou comportamentos envolvendo atividade sexual com uma (ou mais de uma) criança pré-púbere (geralmente com 13 anos ou menos); 2. As fantasias, impulsos sexuais ou comportamentos causam sofrimento clinicamente significativo ou prejuízo no funcionamento social ou ocupacional ou em outras áreas importantes da vida do indivíduo; 3. O indivíduo tem no mínimo 16 anos, e é, pelo menos, 5 anos mais velho que a criança ou crianças (conforme DSM-IV, disponível em: http://www.psicologia.pt/instrumentos/dsm_cid/dsm.php< [Consult. 28 jun. 2013].
45 LEITE, Inês Ferreira - *Pedofilia. Repercussões das Novas Formas de Criminalidade..., cit*., p. 14.
46 GOMES, Francisco Allen/COELHO, Tereza - *A Sexualidade Traída..., cit.*, p. 23.

excecionais; em regra, os menores que aceitam encontrar-se pessoalmente com desconhecidos que conheceram na rede não são petizes, muito menos infantes, mas pré-adolescentes ou adolescentes que, previamente, construíram uma relação telemática de cariz erótica/pornográfica com o "predador sexual", pelo que, quando decidem encontrar-se pessoalmente, fazem-no com consciência (de acordo com a sua capacidade volitiva) e com a clara noção de que vão ter um encontro de cariz sexual[47] (ainda que o façam por uma pluralidade de razões) e, amiúde, revelam amor ou sentimentos íntimos por aqueles. Vítimas que, realço, são, via de regra, pré-adolescentes ou adolescentes, pelo que a temática aproxima-se mais da efebofilia do que da pedofilia, sendo que, deve ser aquela o cerne da preocupação.

Numa segunda instância, se é axiomático que a arquitetura da rede é suscetível de colocar menores em risco, é igualmente verdade que algumas caraterísticas da rede protegem as crianças da vitimação! Desde logo, porque a rede oferece tempo aos menores: não apenas muitos dos meios são assíncronos, o que permite à criança ponderar as suas respostas e ações, como, se pensarmos nos riscos inerentes a contactos pessoais, entre a proposta e o encontro, medeia sempre um tempo, que poderá servir para a criança refletir e mudar de ideias (como, poderá ser usado pelo predador sexual, para controlar os seus impulsos e abster-se de agir). Por outro lado, nas relações *online,* é bem mais complexo para o adulto impor a sua autoridade sobre a criança, ficando esta mais protegida (menos desprotegida). Acresce que a casa continua a ser, para a generalidade das crianças, um local de amparo e segurança, pelo que, enquanto estão a desfrutar de "computadores" em casa (e se os pais exercerem convenientemente as suas obrigações parentais), estarão mais seguras do que algures em parte incerta, fora da vigilância dos seus cuidadores.

Por tudo o que deixei escrito, estou convicto que o abuso sexual perpetrado através da internet é um problema menor quando comparado com outros abusos sobre crianças (nomeadamente os abusos sexuais intrafamiliares) e, não raras vezes, é utilizado como

47 Conforme, WOLAK, Janis [*et al*.] - *Online "Predators" and Their Victims*. "American Psychologist". Washington, p. 113. Especialmente depois da vulgarização das *webcam*, que em muito dificultam a tarefa do predador sexual para escamotear a sua identidade.

narrativa que procura escamotear outras finalidades. Estou em crer que é nímia a "energia, dinheiro e preocupação que dedicamos ao abuso sexual de crianças"[48] na internet.

Como afirmei, no que concerne à internet, os mais vulneráveis são os pré-adolescentes, pelo que importa convocar a questão da efebofilia. Combater a efebofilia pressupõe a compreensão do conceito e exige que cuidemos de saber as suas motivações. Mas, reconheço – porque a temática é pouco trabalhada, porque a mesma se funde nos estudos com a pedofilia –, faltam respostas. Pelo que, as razões que aduzo são perfunctórias: a erotização das crianças e a enfatização dos valores infantis como erógenos explica porque existem tantos adultos que desejam sexualmente adolescentes. Estou convicto de que o combate à efebofilia não se possa construir sem alterar a norma social. As crianças precisam de estabilidade e coerência mas crescem numa sociedade profundamente sexualizada, na qual são quotidianamente expostas a signos sexuais e o prazer erótico surge nos livros, filmes, séries de televisão, músicas e *reality shows*, como o êxtase da felicidade; mas, em casa, os pais tentam domesticar a sexualidade, incutindo-lhes a noção de medo e pecado, pelo que crescem na ambiguidade de desejarem o fruto proibido mas temerem as consequências (sendo que o medo e a curiosidade são os mais importantes estímulos humanos), pelo que, sem atuar sobre a mentalidade dominante, que se alimenta da cultura popular urbana, estamos condenados a fracassar, porquanto, se o combate à efebofilia não dispensa a intervenção punitiva do Estado, não se esgota nesta.

Quiçá a temática que mais deverá inquietar o investigador é o *bulismo*, que humilha, insulta, intimida e ameaça mais de 200 milhões de crianças. E, nem será preciso afirmar, as agressões físicas e psicológicas que estas crianças sofrem têm consequências graves para o seu desenvolvimento psicossocial. No que concerne ao ciberbulismo, estamos perante uma temática que, apesar da propaganda jornalística, é relativamente pouco estudada[49]; se bulismo é um termo utilizado para descrever atos de violência física ou psicológica, deliberados, intencionais e repetidos, praticados por um indivíduo ou grupo de indivíduos, tendo por base uma relação desigual de poder, o ciberbulismo refere-se às

48 KINCAID, James R. - *Erotic Innocence…, cit.*, p. 292 [trad. nossa], que considera, mesmo, ridícula, esta preocupação.
49 Uma boa exceção: FERNANDES, Luís, MORAIS, Tito de, SEIXAS, Sónia – Cyberbullying: Um Guia para Pais e Educadores. Lisboa: Plátano Editora, 2016.

mesmas práticas, quando perpetradas através de um meio telemático. O ciberbulismo é ainda mais capcioso, porque o agressor gosta de ter audiência e a internet oferece-lhe uma (eventual) de milhões de pessoas, que testemunham o achincalhamento da vítima (razão pela qual os agressores sentem prazer em partilhar as ofensas nas redes sociais). Efetivamente, a tecnologia digital permite que os jovens mais populares sejam ainda mais populares e, concomitantemente, que os agredidos sejam ainda mais humilhados. Pelo que, não estranha, muitos atos de *bulismo* são perpetrados especificamente para que as imagens sejam divulgadas na rede.

O ciberbulismo escreve-se com ameaças por telefone ou *email* (ou outras formas de comunicação privada), pela colocação na rede de fotografias (reais ou manipuladas, que pretendem ridicularizar ou envergonhar a vítima), pela remessa massiva de *emails*, o envio de vírus, o sequestro da "personalidade na rede" (através da utilização indevida da palavra-passe do agredido ou criação de perfis falsos), pela criação de blogues/perfis de *Facebook* onde se ofendem as vítimas ou por comentários insidiosos na rede e toda uma extensa panóplia de perversidades que a mente dos mais jovens (e menos jovens, porque, como vimos, existem progenitores colaborantes) tem capacidade para idealizar, porquanto a imaginação da realidade supera toda a ficção.

Se há uma similitude entre o ciberbulismo e o bulismo tradicional, se causas e consequências são semelhantes, distingue-os a possibilidade perversa de o agressor agir cobardemente sob o manto do anonimato; o menor agredido desconhece a identidade do seu agressor, que pode ser um estranho, um conhecido ou mesmo um íntimo (ou simplesmente um *troll*), pelo que, em cada olhar ou sorriso, parece-lhe descobrir um sinal da autoria das agressões cobardes, juntando-se à agressão, este desconhecimento que o atormenta e o deixa inseguro sobre as suas relações sociais, inquieto em saber quem é o seu *inimigo oculto*.

Apressadamente, poderia afirmar que existe uma resposta simples e óbvia para o ciberbulismo: mudar de número de telefone, não frequentar determinados *sites* ou apagar a conta da rede social onde o jovem é atacado. Mas, para um adolescente (ou mesmo para um adulto), a liberdade para se desconectar não é tão simples como utilizar o botão

"apagar"; porque, sair da internet, traduz-se no risco de se tornar um pária, perder a sociabilidade com amigos e conhecidos, bem como, a oportunidade de conhecer novas pessoas. Por outro lado, abandonar não resolve. Não apenas porque o jovem tem a curiosidade, quase masoquista, de saber o que se diz sobre si, como, o facto de não estar na internet, não significa que a internet não esteja na sua vida, nem mesmo que, na sua ausência, não se continue a falar depreciativamente sobre si.

Igualmente preocupante, são os sítios da internet que fazem a apologia da anorexia, da bulimia e do suicídio, para citar os exemplos mais alarmantes. No caso dos sítios *proana*, há uma nota peculiar, que se relaciona com o facto de muitos *sites* que procuram combater a patologia se tornarem numa enciclopédia para candidatos a anoréticos, que utilizam os terríveis relatos das incríveis tolices que adolescentes (e não adolescentes!) fizeram na busca do peso doentio que lhes parece ideal, não como retrato do horror, mas como um repertório de ideias e práticas para testarem. Numa outra dimensão, estes *sites* funcionam como um espaço de partilha, em que os portadores da patologia procuram aceitação e exculpação, sentindo-se parte de um grupo [que, por vezes, parece uma *causa*], bem como, permitem descobrir novas estratégias para perpetuar os seus comportamentos. Por exemplo, é comum encontrarmos fotografias que funcionam como modelos para um corpo "perfeito". Sendo que a estranheza é hipócrita, porquanto, a sociedade criou estereótipos de beleza que tornaram quase obesas símbolos sexuais como Cindy Crawford ou Claudia Schiffer.

Ab initio, assumo que não é fácil determinar se um sítio faz a apologia do suicídio. Se o incitamento ao suicídio é um tipo legal consolidado e com carateres específicos, a noção de apologia do suicídio é fluída e não é fácil identificar o que é um conteúdo pró-suicídio, que exige ser extirpado da rede. As *Mágoas do Jovem Werther*, de GOETHE, que termina com o suicídio do jovem enamorado, incapaz de resistir à impossibilidade de possuir a mulher amada, levou a um aumento dos suicídios nos locais onde foi publicado, tendo mesmo sido proibido em alguns países: colocar este romance na rede, deveria ser proscrito, por incitar ao suicídio?

No que concerne à defesa da automutilação, muitos destes conteúdos estão conexionados com temáticas sexuais, mormente o sadismo e o masoquismo ou com as questões da anorexia e da bulimia, pelo que, *mutatis mutandis*, remeto-me para o que *supra* afirmei sobre estas problemáticas.

Uma outra temática que [alegadamente] preocupa muitos adultos é a cultura de partilha de dados pessoais por crianças e adolescentes; questiona-se se os jovens não foram longe demais, se não estão a partilhar demasiada informação que possa colocar em causa o seu futuro ou que no presente os exponham, quer a predadores sexuais, quer a predadores empresariais, quer à pressão dos pares.

É insofismável que os menores partilham muita informação na internet. Quiçá demasiada informação. E informação suscetível de os humilhar no presente ou no porvir. Como as fotografias que indiscriminadamente disponibilizam no *Facebook*, [*Instagram* e *Snapchat*, porquanto, perante a chegada dos pais, as crianças estão a desertar desta rede social], muitas vezes reproduzindo comportamentos induzidos pelo álcool. Fotografias que ficarão para sempre na rede e que, vinte anos mais tarde, vão ser visionadas pelos seus filhos. Este facto tem feito crescer a convicção, baseada no empirismo, de que os jovens não se preocupam com a sua privacidade (na internet?), que a sua vida privada é partilhada nas redes sociais, construindo a sua sociabilidade de forma despudoradamente pública. Chega mesmo a afirmar-se que vivem a ubiquidade do público e do privado e que a "ideia da existência de duas esferas, uma pública e uma privada é, em certo sentido, um conceito ultrapassado para os jovens de hoje"[50].

Não posso sufragar a tese: os jovens, hoje, são tão ciosos da sua privacidade como os jovens do passado, apenas, "procuram privacidade, como um meio para algo, não como um fim em si mesmo"[51] e têm uma noção de privacidade diferente do conceito dos seus

50 MARWICK, Alice E./DIAZ, Diego Murgia/PALFREY, John - *Youth, Privacy, and Reputation*. [Em linha]. Massachusetts: Berkman Center Research Publication. [Consult. 29 set. 2013]. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1588163<, p. 4.

51 LIVINGSTONE, Sonia - *Children`s Privacy Online: Experimenting with Boundaries Within and Beyond the Family*. In: KRAUT Robert, BRYNIN, Malcolm e KIESLER, Sara - *PC`s, Phones and the Internet: The Social Impact of Information Technology*. Oxford: Oxford University Press, 2006, p. 132 [trad. nossa].

pais (como o conceito dos seus pais não era idêntico à noção dos seus avós, porque, basta recordar as latrinas públicas romanas com vários assentos, em Pompeia, para compreender que a privacidade é um conceito determinado pela cultura), sendo que, mais do que uma *esfera* público/privado, existe uma *esfera* pares/adultos (pais ou professores, mais aqueles que estes), construindo um novo paradigma de privacidade.

Para procurar compreender este fenómeno, importa ter presente que a partilha de informação "privilegiada" faz parte da construção da identidade; aquilo que, por muitos, é entendido como uma intolerável castração da intimidade, é lido como algo normativo nas relações *inter pares* na adolescência: *v.g.*, a partilha da *password* com os namorados ou amigos é interpretada como uma forma de demonstrar fidúcia, que exige reciprocidade, sendo um meio de criar laços e fortalecer as relações significativas interpessoais com os pares, cruciais na adolescência. Os jovens fazem uma verdadeira análise custo/benefício, quando determinam o nível de informação sobre si mesmos que estão disponíveis para partilhar. Existe uma verdadeira guerra silenciosa que os adolescentes travam consigo mesmos na construção da sua "digital *personae*": porque, quanto mais informação e conteúdos são partilhados, maior é a probabilidade de notoriedade e, subsequentemente, de uma maior quantidade de relações pessoais; partilha-se pela necessidade de se ser visto e, também, pela necessidade de ver os outros. Os jovens partilham na internet na procura de popularidade – bem como a possibilidade de mostrar aos outros a sua popularidade – porque a norma social ensina que quanto mais informação se colocar na rede maior número de "amigos" é possível atrair.

Não obstante o que deixei escrito, também creio que os cidadãos, de todas as idades, são demasiado liberais com a informação pessoal disponibilizada, pelo que importa demandar aqueles que mais podem fazer para proteger a privacidade: os próprios. No caso dos menores, porque são estes que me preocupam, urge motivá-los para a necessidade de resguardarem a sua privacidade, explicar-lhes como é que a mesma está a ser violada, incutir-lhes a noção dos riscos, explicando-lhes os perigos; sem uma educação para a proteção, toda a regulação está condenada a fracassar. Tarefa complexa, reconheço-o. Porque raramente somos os melhores juízes de nós próprios. E, quando nos *verdes anos*, falta-nos a maturidade que nos guia para as decisões sábias, pelo que,

compete aos educadores – sejam pais, professores ou outros, com a incumbência de auxiliar no processo educativo de uma criança – alertar para as questões da privacidade. Bem como, trazer à colação o grupo: porque o condicionamento dos pares não está condenado a ser negativo. Porque, a pressão dos pares poderá ser um meio de otimizar cada um de nós, permitindo-nos vislumbrar o que sozinhos não conseguimos ver. O condicionamento não tem inelutavelmente de ser nefasto e acrítico: condicionar os jovens também pode fazer-se pela positiva, com colóquios, aulas e reuniões onde os jovens partilhem experiências, onde se exibam casos concretos na esperança de que, paulatinamente, se altere o paradigma atual e se reforce a consciência da necessidade de resguardar da curiosidade alheia algumas parcelas da privacidade.

Uma outra das (não!) preocupações[52] relacionadas com a internet é o consumo, tantas vezes, obsessivo de jogos de "computador". A escolha provocatória das palavras baseia-se num exame empírico sobre a quase inexistência de estudos sobre a influência da indústria milionária dos jogos eletrónicos para o desenvolvimento psicossomático das crianças.

Quando se reflete sobre estes, é fundamental reconhecer que existem vantagens e desvantagens, pelo que, não é possível esboçar uma análise linear e categórica, porquanto, há componentes destes jogos que são positivas[53], e outras que, provavelmente, são negativas; como, dado que é uma realidade imberbe, e pela dificuldade fática em realizar estudos[54], é impossível perceber quais os efeitos a longo prazo. Em defesa dos benefícios

52 Faço a ressalva, porquanto importa não obliterar que crucificamos os jovens por consumirem massivamente jogos (e jogos com graus *pornográficos* de violência gratuita), mas que estes são produzidos por adultos e, via de regra, adquiridos por pais e outros educadores, também eles adultos, quiçá os mesmos, que depois blasfemam contra os critérios estéticos dos jovens.

53 A melhor defesa dos aspetos positivos dos jogos de computador é a apresentada por JOHNSON, Steven - *Everything Bad Is Good For You: How Popular Culture Is Making Us Smarter*. New York: Riverhead Books, 2005, *passim*.

54 A base académica para a consagração da noção empírica da perigosidade para as crianças das imagens violentas foi apresentada por BANDURA, ROSS e ROSS, no início da década de sessenta, que tendo por objeto crianças entre os 8 e os 13 anos a quem eram exibidas imagens nas quais um adulto abusava de um boneco com aparência humana, dividiram o cuidado de crianças pequenas entre os jovens que tinham visto e os que não tinham visionado as imagens *supra* referidas, sendo que o grupo que as observou demonstrou maior agressividade e intolerância para com os mais petizes (BANDURA, Albert/ROSS, Dorothea/ROSS, Sheila A. - *Transmission of Agression Through Imitation of Aggressive Models*. *In*: "Journal of Abnormal and Social Psychology". Washington. v. 63, pp. 575 e ss.).
Com *data venia*, o estudo não parece permitir conclusões definitivas: porque nem sempre é exequível realizar algumas experiências com crianças, como não podemos fechá-las num laboratório durante uma

dos jogos, afiança-se que estes são desafios cognitivos que desenvolvem a capacidade de raciocínio, o espírito colaborativo, a sociabilidade, melhoram a competitividade, e que, se desejamos aquilatar as suas vantagens, não podemos cingir a nossa análise ao seu conteúdo. E que, tem sido esta visão redutora que tem fundamentado o pensamento apocalíptico, porquanto, as vantagens dos jogos são invisíveis a uma interpretação a "olho nu"; da mesma forma que, do facto de a maioria das pessoas não aplicar a álgebra no seu quotidiano, não legitima concluir pela sua irrelevância, também os jogos permitem desenvolver aptidões físicas e mentais, muito além da apreciação ao seu conteúdo.

Começo esta sucinta análise por deixar cair falsos dogmas, ardilosamente construídos para tranquilizar quem deveria estar intranquilo; é uma falácia acreditar que estes jogos *online* promovem a sociabilidade; mesmo quando os jovens jogam em grupo, presencialmente ou à distância, os parceiros funcionam, quase sempre, como autómatos; como, é irreal acreditar estarmos perante uma forma de entretenimento que fomenta a liberdade do jogador, porque todas as suas possibilidades estão predeterminadas na programação do jogo. A narrativa de que estes jogos contribuem para o desenvolvimento cognitivo, para as capacidades motoras, e que funcionam como uma preparação para os desafios do mundo digital capacitando-os para a *e-sociedade*, também não pode aceitar-se acriticamente. Com efeito, o consumo excessivo de jogos virtuais, não apenas poderá ser um propulsor de isolamento, uma síndrome do filho único, que através dos jogos constrói uma fuga da realidade, como promove uma alienação perante a realidade que o circula, sendo, ainda, recorrente a alegação de uma verdadeira compulsividade e mesmo adição. Acresce, o receio dos efeitos psicológicos de alguns jogos virtuais, passíveis de gerar nas crianças uma incapacidade para distinguir a realidade da ficção ou para lhes incutir impulsos violentos.

década, expô-las a riscos, asséticas a outros estímulos, para nos oferecerem a certeza certa de quais as reais consequências do seu consumo obsessivo de jogos. Até porque, sobre este tipo de temáticas, os estudos estão preenchidos por lacunas; colocar crianças a visualizar um filme violento enquanto outras ficam a ver um filme não violento, para concluir que a visualização daqueles conteúdos torna as crianças mais agressivas, é falacioso. Porque as crianças que visualizaram ambos os filmes não cresceram num laboratório nem numa ilha isolada, porque a suposta agressividade demonstrada pode ter uma panóplia de diferentes motivações.

Destarte, um debate sobre as maléficas consequências para as crianças da internet em geral e dos jogos virtuais em particular ficaria ameaçado, se não fosse abordada a querela da exposição das crianças à violência, uma obsessão cada vez maior, que parece procurar escamotear a existência de questões mais prementes, procurando, simplisticamente, uma relação direta, obrigatória, um *post hoc ergo propter hoc* entre o acréscimo de violência nas televisões, cinema, jogos de computador, e o aumento da criminalidade juvenil. O fantasma da criança brutalizada pela irracionalidade cruel e bruta dos meios de comunicação convive connosco e está mais manifesta do que nunca com o advento da internet e do digital, que deixam a criança exposta à voracidade dos produtores de conteúdos e de todos aqueles que os distribuem. Receia-se a violência nos meios de comunicação porque se receia a criança. Teme-se a violência imitativa porque se teme a criança. Preocupações que têm como pressuposto uma "noção pós-romântica da criança inocente e vulnerável que precisa ser protegida das influências não-naturais do mundo adulto. No entanto, subjacente a esta ideia, está uma visão muito mais antiga, a da criança como portadora do pecado original. Nessa perspetiva, as crianças são "naturais" não em sentido positivo, mas em sentido negativo: têm inclinações para a violência, sexualidade e comportamentos antissociais que são difíceis de controlar (e que as influências irracionais dos *media* teriam o poder de liberar)"[55].

Dessarte, sem pretender desprezar aqueles argumentos como uma hipérbole vazia, a premissa não pode absorver-se sem cuidada reflexão: se um bando de adolescentes reproduz uma cena violenta que consumiu no cinema, na televisão ou num videojogo, não se pode, apressadamente, culpar o meio, antes, importa questionar se essas imagens violentas não habitavam já dentro de si, se no seu interior não transportavam outras cenas de violência que vivenciaram, bem como o desejo vil de as colocar em prática.

A discussão sobre a exposição dos jovens à violência é longa e não gera consensos[56]; concomitantemente com os estudos que confirmam que os jogos violentos promovem violência, não apenas, há estudos que "provam" não existir relação entre o

55 BUCKINGHAM, David - *Crecer en la Era de los Medios Electrónicos, cit.*, p. 142.
56 Aliás, discute-se, mesmo, se a própria Bíblia não é demasiado violenta para ser consumida por crianças (conforme CUNHA, Paulo Ferreira da - *O Ponto de Arquimedes: Natureza Humana, Direito Natural, Direitos Humanos*. Coimbra: Livraria Almedina, 2001, p. 187).

aumento da violência e o consumo de jogos violentos, pelo que estes seriam neutros, como, surgem estudos cujas conclusões apontam para os efeitos positivos dos jogos violentos nos jovens, ajudando a amenizar o seu comportamento agressivo, "que as experiências violentas vivenciadas ao longo do jogo podem resultar em sentimentos positivos por meio da ocorrência de catarse"[57]. Até porque, quando analisadas, as reações dos consumidores de produtos violentos, estes tendem a ter uma muito maior empatia com as vítimas do que com os perpetradores de comportamentos violentos, o que pode sugerir que, contrariando o senso comum, o visionamento de imagens violentas é suscetível de mitigar os comportamentos violentos e propiciar uma melhor adequação ao cumprimento do normativo social, pelo que, este consumo seria benéfico para o menor, porquanto, funciona como uma purgação emocional, que permite uma satisfação indireta dos desejos violentos, e substituindo-se o consumo de violência pela prática da violência. Além de que, na maioria dos conteúdos qualificados como violentos, encontramos a vitória do *bem sobre o mal* e a enfatização de valores morais que são benéficas para o salutar desenvolvimento infantil.

Por outro lado, nesta discussão, escamoteia-se que a mais vil violência que corrompe os jovens não surge nos filmes do cinema, nas séries de televisão, nos jogos de computador, antes surge, pontualmente, às horas certas dos noticiários, o terror da realidade, tantas vezes explorado por fins comerciais pelo sensacionalismo abutre do quotidiano [a masturbação da dor, como se lhe refere José Pacheco PEREIRA]. Porque, o embate da violência, mais do que as especificidades das imagens e o seu concreto teor, tem um maior impacto e uma perigosidade mais acentuada quando surpreende o espectador, quando surge num momento, num local ou num contexto, em que não eram expectáveis tais imagens.

Quanto a mim, não tenho dúvidas em frisar que procurar cingir a problemática do crescimento da violência juvenil (que existe!) aos conteúdos que lhe são servidos através

57 Assim, GREENFIEL, *apud* SI SILVA, Rosane Leal - *A Proteção Integral dos Adolescentes Internautas: Limites e Possibilidades em face dos Riscos do Ciberespaço*. [Em linha]. Florianópolis: Portal do Domínio Público. [Consult. 12 Nov. 2012]. Disponível em: http://www.dominiopublico.gov.br/pesquisa/DetalheObraForm.do?select_action=&co_obra=157368<, p. 172.

dos jogos e da internet é uma solução errática, porque redutora, que carrila o risco de absconder que o problema da violência é multifacetado.

Os eventuais riscos para os menores decorrentes da violação dos direitos de propriedade intelectual não merecem mais do que um parágrafo da minha atenção. Não que abrace as teses de que *de minimis non curat praetor* ou que esta é inócua ou, ainda, que são uma reação política contra as práticas oligárquicas do modelo de negócio das grandes editoras que merece ser encorajada ou que os direitos de autor sejam um instituto obsoleto; não merecem mais que uma referência fugaz, porque a realidade portuguesa não expõe os menores às (absurdas) medidas punitivas de outros ordenamentos jurídicos, como o espaço jurídico americano, como entendo que as editoras, em *pseudo-representação* dos autores, já trilharam os caminhos necessários, pelo que, de uma perspetiva teórica, será um problema menor.

A exposição das crianças às práticas comerciais abusivas não tem especificidades, em relação à sujeição dos adultos às mesmas práticas (com exceção da vulnerabilidade acrescida de quem é mais débil); mas, refira-se, se as crianças tivessem memórias dos primeiros instantes de vida extrauterina, a sua primeira imagem do mundo seria a múltipla publicidade que inunda as maternidades, toda uma panóplia de bens que se assumem como indispensáveis para a sobrevivência e bem-estar dos recém-nascidos. Chegadas a suas casas, o centro da vida familiar é uma televisão que vomita publicidade continuamente; quando começam a ter noção de si mesmas, as crianças são confrontadas com outras crianças, que brincam, pulam e sorriem nas nossas televisões, agarradas a brinquedos e a tantas outras desnecessidades necessárias da modernidade, convidando-as a alcançarem a felicidade através daqueles produtos. As escolas estão hoje inundadas por *marcas*, que estabelecem fronteiras intransponíveis entre aqueles que as podem adquirir e os outros. E, algures, entre as empresas e as crianças, os pais vivem nesta ambivalência, entre a consciência dos malefícios do consumismo e a ânsia de satisfazer os desejos dos seus petizes. Reconheça-se a genialidade: formatar as crianças desde a idade da inocência para as delícias do consumismo, mercantilizar a infância, permite garantir toda uma geração de obcecados pelo consumo. Acresce que, nunca como no presente, as crianças tiveram uma palavra tão ativa nas decisões aquisitivas das famílias e consumiram tantos

recursos financeiros aos seus pais, que, não obstante terem sido afastadas da produção económica, estão no cerne da produção de recursos económicos: nunca as crianças "custaram" tanto dinheiro, se a crueldade da expressão me é admitida[58]. A cultura de consumo dirigida às crianças é um tema pouco explorado entre a mais egrégia doutrina. Os autores que se debruçam sobre o tema tendem a digladiar-se entre a alegação da inocência das crianças que são subjugadas aos interesses corporativos, que condicionam as suas escolhas, e aqueles que enaltecem a autonomia das crianças, que lhes permite satisfazer os seus interesses, cuja informação e propaganda abundantes lhes dá poder de escolha. Permita-me o leitor que seja incisivo: se a publicidade não nos influencia, importa informar as empresas que, neste caso, andam a desperdiçar milhões em publicidade.

Em tom de conclusão, quando pensamos na soma de todos estes perigos, temos a tentação de concordar com o arcebispo WULFSTAN quando, num sermão proferido em York, vaticinou que "o mundo está a aproximar-se velozmente do fim"[59]. Mas o mundo não acabou e, 1000 anos depois, escrevi uma dissertação sobre novos perigos[60]. Não sou hipócrita: expor crianças, e mesmo adolescentes, a imagens nocivas, vivenciar traumáticas experiências de *cyberbullying*, expô-las prematuramente à pornografia, serem vítimas de pedofilia, é suscetível de provocar graves danos aos menores; mas, reconhecer os perigos não é contribuir para a ciberfobia histérica e sugerir que coloquemos os aparelhos tecnológicos dos nossos filhos numa fogueira. Porque se a internet tem perigos e riscos, importa recordar que *ainda é possível escrever poesia depois de Auschwitz*.

58 Segundo dados do Instituto Nacional de Estatística, ter um filho tem encargos anuais de cerca de 10 mil Euros (*vide Ter filhos custa 10 mil euros por ano aos pais* (26 jun. 2012). "Correio da Manhã". Disponível em: http://www.cmjornal.xl.pt/detalhe/noticias/exclusivo-cm/ter-filhos-custa-10-mil-euros-por-ano-aos-pais<); este dado permite-me sufragar as palavras de BAUMAN, quando escreve "que os filhos são as aquisições mais caras que o consumidor médio pode fazer ao longo de toda uma vida. Em termos puramente económicos, eles custam mais do que um carro luxuoso do ano, uma volta ao mundo em um cruzeiro ou mesmo uma mansão" (BAUMAN, Zygmunt - *Amor Líquido: sobre a Fragilidade dos Laços Humanos, cit.*, p. 29).

59 De impressionante na frase apenas o singelo facto de ter sido proferida em 1014, o que ilustra que o pessimismo sobre o futuro da humanidade não é uma caraterística coeva (conforme GIDDENS, Anthony - *O Mundo na Era da Globalização, cit*., p. 15).

60 Refiro-me a LANÇA, Hugo Cunha – *A Regulação dos Conteúdos Disponíveis na Internet: a Imperatividade de Proteger as Crianças*. Lisboa: Chiado Editora, 2016, obra que está na base deste artigo.

3. O QUE É UMA CRIANÇA?

Escalpelizar o tema exige-se porque o acesso dos jovens cidadãos à internet cresceu desmesuradamente nos últimos anos, abrindo novas avenidas para a comunicação, novas formas de adquirir, processar e distribuir informação, numa opulência comunicacional cujos efeitos ainda não apreendemos na globalidade, mas que, hoje já sabemos, não serão incólumes. E a obsessão pela modernidade, aliada a um deslumbramento tecnológico, permitiu que a internet entrasse na vida dos infantes, sem existirem estudos sólidos que permitissem uma opinião fundamentada, tornando os *nativos digitais* cobaias do experimentalismo social, cujas consequências apenas daqui a décadas será possível aferir.

Mas, mesmo na incerteza, posso constatar algumas certezas.

Desde logo, a internet permite que, de uma pequena aldeia, a criança possa ver todo o universo, *pelo que, a sua aldeia vai ser tão grande como outra terra qualquer e a criança vai ser do tamanho do que vê, não do tamanho da sua altura*; o problema é que, porque os educadores perderam a capacidade para filtrar a informação a que a criança acede, esta é exposta a amálgamas de conteúdos díspares, que nem sempre tem capacidade para processar. Porque, se a internet é uma complexa cidade eletrónica, também é composta por muitas aldeias. E, se algumas destas aldeias se assemelham à *Terra do Nunca* e permitem que as nossas crianças brinquem com o *Peter Pan* e os *meninos perdidos*, outras aldeias são inóspitas, potencialmente perigosas, desaconselhadas a crianças de todas as idades. Mas, não obstante, estas aldeias também são habitadas pelas nossas crianças. Porque, se consideramos que os perigos são inflamados, é preciso ter consciência de que há predadores sexuais que se alimentam da internet, que há *sites* que perfilham o suicídio, que promovem a anorexia e a bulimia, que o bulismo é uma realidade cada vez mais premente na rede, que a liberdade incontida de expressão pode ter consequências nefastas, e que nem todos os jogos são brincadeiras inocentes. Mas, se avoquei os riscos, procurei desconstruir as fábulas que navegam no imaginário coletivo sobre a internet; como sublinhei, a ubiquidade de sentimentos sobre o desconhecido êxtase/medo explica os mitos exacerbados que se construíram sobre os malefícios da internet para as crianças. Até porque, não é a tecnologia que maltrata as crianças: são as pessoas.

Todavia, todas estas preocupações que evoquei, convocam uma pergunta. Uma questão que parece pueril, mas Milan KUNDERA está certo quando nos diz que *as perguntas realmente sérias são apenas aquelas que uma criança pode formular. Só as perguntas mais ingénuas são realmente perguntas sérias*[61]: o que é uma criança?

Dessarte, porque o objeto deste estudo tem como sujeito as crianças, é imprescindível cotejar o conceito de criança (o que é ser criança no século XXI?), quantificar o conceito (até que idade se é criança?) e compreender o seu significado, densificando-o pelo confronto com os dados oferecidos pela história e pelas mais recentes correntes da sociologia e da psicologia, de molde a procurar compreender como o Direito interpreta as crianças e validar um novo campo discursivo da infância, através de uma reflexão jurídico-social, moralmente fundamentada, mediante uma meta interpretação de tempo e de lugar e tendo como perspetiva a civilização jurídica ocidental [porque não caí no logro de pensar que todas as crianças vêm ao mundo da mesma maneira: os perigos a que as crianças portuguesas são expostas são, incomensuravelmente, diversos daqueles que afetam as crianças *africanas*[62], sendo que, assumindo o *pecado* do eurocentrismo, será este o paradigma que domina as nossas cogitações. Porque, se a internet é global, as crianças não].

Ciente de que os textos normativos nacionais e transnacionais apontam para uma classificação com base no critério objetivo da idade, que se prolonga até aos 18 anos, num maniqueísmo que separa a menoridade da maioridade, entendo que o mesmo não corresponde ao *interesse superior da criança*, pelo que, exige-se, do intérprete, um esforço para considerar cada criança *de per si* e não como uma mera parte disforme de um todo uniforme. Como, não podemos insistir numa visão dicotómica entre crianças e adultos, escamoteando o surgimento de um *tertium genus*, a adolescência, caracterizada por uma mescla de independência e dependência, com uma maturidade muitas vezes imatura, mas um ser com a sua ipseidade, pelo que não pode continuar a ser interpretada

61 *In:* A Insustentável Leveza do Ser.
62 Quando me refiro a África, não usamos a expressão como um continente, como um espaço geográfico, mas como um conceito.

como um "há-de ser" em abstrato, mas como um "ser" concreto, de forma assistemática e casuística. Um "ser" único com a sua ipseidade, que não pode continuar a ser analisado através de grilhetas paternalistas.

Brevitatis causa, desde logo, importa dividir a menoridade entre nascituros, que são as crianças até ao momento do parto, infantes, os menores até aos seis anos, petizes, os que estão compreendidos entre os seis e os doze anos, idade em que os menores começam a ser responsabilizados pelo desvalor dos seus atos, no âmbito da lei tutelar educativa, pré-adolescentes, os maiores de doze anos, compreendendo que no estádio da civilização atual os menores desenvolvem mais cedo a sua autonomia, sendo esta uma etapa de relativa maturidade, que ainda exige ser tutelada e, por fim, adolescentes, os maiores de 16 anos e menores de 18 (ou 21).

Por outro lado, e por mais que contraste com os arquétipos escritos nos desgastados livros da parentalidade, importa reconhecer que o discernimento funciona como um *status* liberatório que alforria o adolescente das grilhetas da submissão à autoridade parental.

Por anátema que seja para uma pauta mais conservadora da educação, hoje impõe-se reconhecer às crianças [quando entram na idade da razão] liberdade para impor a quem exerce a autoridade parental o seu modo de vestir, o corte de cabelo, colocar um *piercing* interno ou externo, fazer tatuagens, colocar um alargador de orelhas, inscrever-se numa associação ou partido, escolher a sua própria religião ou assumir-se como ateu, agnóstico ou abraçar o islamismo, decidir continuar ou interromper uma gravidez, permitir ou proibir tratamentos médicos, fazer escolhas sexuais, selecionar que desportos pretende praticar, deliberar se pretende receber informação sexual e utilizar contracetivos, se quer publicar as suas obras, bem como, para trazer à colação as temáticas que diretamente se relacionam com este estudo, ter uma página numa rede social, criar um blogue, expor fotografias suas de cariz pessoal ou íntimo, consumir erotismo ou pornografia, publicar na rede obras artísticas e quaisquer outras das inúmeras e heterogéneas condutas que a internet oferece aos menores e maiores. Porque, as crianças não são necessariamente *Jack Merridews*, nem habitam na ilha *do Deus das Moscas* e, importa nunca esquecer, os pais têm de educar os filhos que têm, não os que gostavam de ter…

4. O QUE É PROTEGER?

Se queremos proteger as crianças, uma questão prévia é indagar sobre o estatuto epistemológico de proteção, dada a equivocidade do conceito, e cogitar se proteger significa colocar a criança numa redoma imune às misérias do mundo ou, pelo contrário, esta constrói-se quando as crianças são expostas a conteúdos que, apesar de inconvenientes, fazem parte da vida, ensinando-a a lidar com o abjeto, fornecendo-lhe informação e ferramentas emocionais para lidar com o lado ignóbil da vida?

Acredito que, para a operacionalização do conceito, é preciso derrotar fantasmas (pseudo) pamprotecionistas e reconhecer que o desenvolvimento integral das crianças necessita de uma margem de transgressão. Sem cair nas falácias do adultocentrismo, antes, partindo da premissa da criança enquanto pessoa, tendo bem presente que "nenhum de nós é suficientemente filósofo para saber pôr-se no lugar de uma criança"[63]; em defesa desta opinião, furtei as palavras de José Luís PEIXOTO quando ensina "eu tive catorze anos, mas não tive os teus catorze anos. Tive os meus. As dúvidas eram diferentes e, quando é assim, as certezas também variam"[64].

Sufrago que proteger não é fechar as crianças numa redoma e acreditar que podem crescer sem conhecer o lado abjeto da vida [porque, recordo, mesmo no Jardim do Éden habitava uma serpente], pelo que se exige amenizar o exacerbado cunho tutelar e enfatizar a valência da preparação para a vida adulta: porque o crescimento constrói-se com espaços de liberdade e, também, se faz com erros, com transgressões [porque só a errar, se pode errar melhor, para recordar a profecia de BECKETT]. Como, evoco a imperatividade da interiorização do conceito do menor enquanto pessoa em desenvolvimento, compreender que a infância (e particularmente a adolescência) não é apenas um estado transitório para a idade adulta, mas uma fase da vida, com caraterísticas próprias, pelo que se impõe o reconhecimento da sua esfera de autodeterminação, tendo

63 ROUSSEAU, Jean-Jacques - *Emílio*. Trad. Pilar Delvaulx. Mem Martins: Publicações Europa-América, 1990, p. 112.
64 PEIXOTO, José Luis - *Abraço*. 8.ª Ed. Lisboa: Quenzal Editores, 2012, p. 155. Uma reflexão semelhante, tendo por paradigma a cultura dos jogos virtuais, é oferecida por CARDOSO, Gustavo - *E-Generation: Os Usos de Media pelas Crianças e Jovens em Portugal*. Lisboa: CIES/ISCTE, 2007, p. 223.

como limite interno a sua autonomia volitiva. Tenho consciência que algumas das soluções preconizadas ferem o senso comum; defender a autonomia dos adolescentes, a obrigatoriedade de os pais respeitarem filosofias, gostos e práticas heterogéneas, sustentar que, mesmo na infância, existe o direito a seguir o próprio caminho (mesmo quando se escolhe uma estrada repleta de perigos), e que os pais ficam na situação inelutável de respeitar escolhas que abominam, colide com a visão ainda maioritária do exercício da parentalidade. Porque o conceito de família democrática ainda é interpretado como um [perigoso!] esoterismo sociológico. Porque, não escamoteio, as palmadas pedagógicas parecem uma solução mais eficiente (e de certeza mais simples), que o diálogo e s negociação com os petizes. Porque o androcentrismo que relaciona a dependência económica com o exercício da autoridade, ainda está inculcado no ADN da sociedade, traduzindo-se num *argumentum ad baculum*.

Não tenho dúvidas que o exercício da parentalidade no século XXI é muito mais complexo do que em qualquer período histórico anterior. Como, era muito mais simples ser marido antes do *25 de Abril*, quando as relações extraconjugais masculinas eram socialmente aceites e juridicamente inócuas, quando o marido determinava se e onde a mulher podia trabalhar, tinha o direito de depósito, o poder de correção e a autonomia financeira do património conjugal. Como, historicamente, era mais fácil ser europeu caucasiano e ter o direito de colonizar, escravizar e aniquilar outras raças e explorar os territórios em todo o mundo. Como, na Europa era muito mais simples ser católico e ter o direito de evangelizar, através do saque e da perseguição, quem cultivava outros credos. Porque houve um tempo em que o direito e a arquitetura social eram unânimes em consagrar a superioridade do homem, caucasiano, europeu e católico, porque mulheres, negros, índios e hereges eram seres inferiores, incapazes de cuidar de si e dos seus interesses, carentes da tutela protetora dos outros, que tinham todas as respostas e sabiam o que era o melhor para proteger os mais frágeis: o *fardo do homem branco*[65].

O desafio coevo é estimular os jovens para a liberdade, pugnar para que estes construam a sua autonomia intelectual, social e afetiva, para que sejam os escritores das suas histórias, os protagonistas das suas vidas. O que conduz a uma nova pergunta

65 Referimo-nos ao poema de Rudyard KIPLING.

fundamental: como fazê-lo? Especialmente num tempo em que os *curricula* escolares se tornaram num mecanismo para controlar a informação a que as crianças têm acesso, um meio de formatar cérebros e evangelizar os alunos de acordo com as correntes ditas maioritárias, em que a educação se tornou um concurso, onde o saber é escrutinado como um jogo, em que o sucesso de um modelo educativo se afere pelas percentagens num exame nacional (pelo que não se cultiva o gosto pelo saber, mas a exigência de resultados, através da memorização, não do conhecimento), é temerário confiar no ensino formal para criar jovens com mente livre, aberta e criativa.

Por tudo, defendo que a incapacidade genérica de todos os menores cuidarem de si é uma falácia que urge desconstruir e que colide com princípios axiológico-constitucionais; como, sustento que a menoridade não pode ser interpretada como uma realidade una, sendo indispensável que seja escalonada por idades referência. Com o devir da idade, aumenta o espaço de autonomia do menor e contrai o conteúdo da autoridade parental, sendo que, na adolescência, é injustificável a manutenção do instituto da representação legal. O que não significa abandonar as crianças aos seus direitos. Porque da mesma forma que os adultos não deixam de aconselhar-se junto de familiares, amigos e especialistas, reconhecer autonomia às crianças não significa que estas atuem juridicamente de modo assético. As novas crianças podem ser uma *e-generation*, mas, no final do dia, como ensinou o poeta, *metade das crianças é amor e a outra metade...também*, pelo que os princípios e valores que os pais lhe transmitem durante o crescimento fazem parte da sua essência.

5. COMO REGULAR A INTERNET?

Para dar resposta ao quesito, é crucial revisitar as premissas dos ciberlibertários, para valorar criticamente as mesmas. O seu pensamento foi dominante aquando da génese da rede e as suas hipóteses e teses continuam a influenciar quem se debruça sobre o tema. Dessarte, quando mergulhamos na história da história da internet, constatamos que os seus primórdios se caracterizaram por uma anarquia organizada, tendo por diretrizes as posições dos seus *founding fathers*; foi um tempo em que se acreditava que *paus e pedras* poderiam magoar mas que os *bytes* eram inócuos. Por outro lado, se um habitante do

ciberespaço sentisse os seus direitos violados, teria sempre a possibilidade de abandonar aquele ambiente da rede e procurar outro, com valores semelhantes aos seus, ou, simplesmente, despir-se do seu *nick*, vestir novas roupas e regressar com um novo rosto.

Mas a democratização da internet provou que era um sofismo acreditar que a rede era um mundo em que a regulação era despicienda. Uma primeira resposta foi Acreditar que os habitantes deste novo mundo seriam os agentes normogenéticos com legitimidade e capacidade para regular as suas relações recíprocas; e, justificaram-no argumentando, que os Estados não tinham conhecimentos para regular a internet, que não tinham legitimidade, que eram impassíveis para impor o cumprimento das suas leis. Premissas que é importante desconstruir. Até porque, o desenvolvimento da internet tornou-se a Némesis que traiu a utopia dos seus criadores; não apenas a tecnologia pode ser uma aliada dos Estados, como a democratização da rede, tornou a presença dos poderes públicos numa inevitabilidade.

Reconhecer a necessidade de regulação estadual é apenas uma aporia para novos problemas. *Ab initio*, se a nossa missão é procurar regular os conteúdos disponíveis na rede, é crucial refletir sobre o que pretendemos que seja a internet; porque, se regular é estabelecer um conjunto de regras cuja observância se considera imperativa para a convivência social, porque os Estados têm o direito de proteger o que são e o que desejam ser e "um acto não ofende a consciência porque é criminoso, mas é criminoso porque ofende a consciência comum"[66], regular também é dirigir, também é determinar uma orientação, pelo que é fundamental perceber qual o caminho que desejamos seguir, porquanto, como SÉNECA nos ensinou, *nenhum vento sopra a favor de quem não sabe para onde quer ir*. E fiz a minha escolha! Estou convicto que a regulação é [deverá ser!] um meio para garantir uma internet democrática, que não seja um couto dos interesses de alguns (poderosos) Estados, presa a corporações ou subjugada aos interesses comerciais de algumas empresas, antes, uma comunidade de cidadãos, com respeito pelas idiossincrasias de cada povo, em que os princípios democráticos que regem a(s) nossa(s) coletividade(s) não se extinguem na extremidade de um *modem*.

66 DURKHEIM, Emile - *A Divisão do Trabalho Social*. V.1. 3ª Ed. Trad. Eduardo Freitas/Inês Mansinho. Lisboa: Editorial Presença, 1989, p. 100.

Para alcançar o desiderato, importa ultrapassar um conjunto de ambiguidades que têm oferecido constrangimentos aos legisladores, nacionais e internacionais, quando procuram concretizar a sua missão. A primeira ambiguidade é compreender a imperatividade de proteger a privacidade do utilizador, contra o *voyeurismo* de particulares, empresas e Estados [não sendo lícito ao académico atemorizar-se pelos receios reais e efabulados dos *11 de Setembro* deste mundo], mas, reconhecer que, em determinados casos, o conteúdo axiológico jurídico-constitucional da privacidade poderá colidir com outros princípios fundamentais, pelo que se exige uma valoração crítica, porquanto a intransigente defesa da privacidade não é, nem pode ser, conflituante com a responsabilização dos infratores (outro pilar das minhas cogitações).

A liberdade de expressão é outra ambiguidade que o intérprete enfrenta amiúde e que tem sido seara profícua de ilicitudes, porquanto, tem sido uma forma disruptiva para atacar a honra alheia por aqueles que anonimamente invadem a rede e que procuram, agitando o manto da espessura constitucional da liberdade de expressão, escapulir-se à responsabilização pelos seus atos: se a liberdade de expressão é um valor fundamental que exige proteção, não pode ser endeusada como um valor em si mesmo, absoluto, incondicional. Trago o tema à colação, porque um dos mais complexos problemas atinentes à regulação da internet relaciona-se com o controlo da qualidade da informação que navega na rede, digladiando-se correntes contraditórias, um diálogo *surdo* entre os defensores do controlo qualitativo da informação, sufragando que os Estados têm legitimidade para impedir a circulação de determinados conteúdos (*inter alia*, a pornografia, a pedofilia, p incitamento ao ódio) e os apologistas da abordagem *laissez-faire,* crentes que a informação em circunstância alguma deverá ser regulada, que podemos confiar na mão invisível[67], porque a boa moeda de GRESHAM vai permitir expulsar a má informação da internet. *Ab initio* assumo, sem eufemismos, que defender que determinados conteúdos são proscritos e que devem ser excomungados da rede, é defender a censura. E, não escamoteio, defender a censura, *v.g.* da pedopornografia, é destapar a caixa de Pandora, não estivesse a história da censura pejada de boas intenções; porque, não ignoro, os mesmos mecanismos e técnicas que construirmos para impedir

67 Mas importa recordar que, muitas vezes, a mão apenas é invisível, porque escolhemos olhar para o outro lado e não ver a mão que (não) embala o mercado...

que estes conteúdos naveguem na internet podem ser usados [são usados] para censurar ideias e pensamentos. Mas escolher é optar: e a minha opção foi esta. Porque "o nosso amor à liberdade não deve levar-nos a negligenciar os problemas ligados à utilização abusiva da liberdade"[68]. E, em apoio das minhas convicções, chamo à colação o teórico da sociedade aberta que declarou "infelizmente é necessário recorrer à censura"[69].

Vencidas as primeiras querelas, novas aporias ensombram o horizonte; a realidade historicamente construída ensinou-nos que regular conteúdos na internet suscita especificidades que o intérprete não pode ignorar: por regra da experiência, assumo que não é fácil subsumir as condutas praticadas na rede ao ordenamento jurídico de um determinado Estado. A transnacionalidade e a desterritorialização da internet permitem que alguém em Portugal coloque uma informação num *site* brasileiro, sobre acontecimentos ocorridos em Paris, com cidadãos ingleses, que, posteriormente, será replicada através de *mirrors* e deslocalizada para servidores imunes ao *ius imperii* dos Estados em cotejo; também a desmaterialização não é alheia a angústias e oferece aporias específicas; por fim, a questão do anonimato (ilustrada no inesquecível *cartoon* de Peter STEINER publicado no *The New Yorker*, em 1993, com a frase "na internet ninguém sabe que és um cão"), não apenas dificulta a responsabilização, como, parece fazer esfumar a cordialidade que norteia as relações interpessoais, estimulando a *incivilidade*, em pessoas que jamais teriam semelhante conduta *a latere* da, alegada, penumbra oferecida pela rede [porque o anel de Giges existe e vive na internet].

Acresce que, como se os problemas *supra* expostos não fossem, suficientemente, periclitantes, a querela da regulação dos conteúdos tem de ser interpretada num contexto de crise do Direito estadual, tendo por premissa a contradição, aparentemente inconciliável, de uma organização sociopolítica submergida aos ditames do princípio da territorialidade e o facto de que muitos dos mais prementes desafios coevos não serem *geolocalizados*, antes, extravasam fronteiras, para se assumirem como problemáticas globais, como, *inter alia*, a proteção do ambiente, a luta contra o terrorismo, o tráfico de droga e pessoas, a globalização económica (e a governança da internet).

68 POPPER, *apud* BOSETTI, Giancarlo - *Introdução*. *In*: POPPER, Karl/CONDRY, John - *Televisão: Um Perigo para a Democracia*. 4ª Ed. Trad. Maria Carvalho. Lisboa: Gradiva, 2012, p. 10.
69 *Ibidem*, p. 7.

Indubitavelmente, a globalização é um constrangimento à capacidade dos Estados para imporem a sua soberania, inquinando as democracias, enunciando o fim do unilateralismo, confrontando os Estados com o *dilema do prisioneiro*, porquanto, as suas decisões são suscetíveis de afetar os nacionais de outros Estados e vincular cidadãos que não contribuíram para a formação da vontade política estadual ou, em caso de omissão, ofender as pretensões dos seus concidadãos. Pelo que, o Direito está a mudar e "nem há que estranhá-lo, pois o direito não podia decerto ficar imune na complexa crise moral e cultural que é a nossa circunstância"[70].

Reconhecer que os Estados têm armas para impor a sua vontade não é sufragar uma visão totalitária da Lei na rede mundial de computadores. Porque se a Lei é necessária, não acredito que seja suficiente. Dessarte, defendo que a corregulação deverá ser o paradigma da regulação da internet, através do reconhecimento de que, para regular a rede, é preciso conjugar as diversas modalidades de autorregulação com a regulação estadual e apelar à cooperação internacional.

Dessarte, interpreto o Direito como parte do universo normativo[71]; não acredito que o ordenamento jurídico tenha, quer a valência, quer a capacidade, para regular a sociedade globalmente, pelo que, subscrevo, a par da Lei, importa enaltecer outros modelos regulatórios, abraçando uma visão holística para a regulação dos conteúdos disponíveis na internet. O que contrasta com o positivismo legalista triunfante que tem a tendência para assumir que a regulação é uma atividade do Estado, ignorando outras formas de regulação, e duvidar de "um controlo informal por sobrolho franzido à margem de qualquer heteronomia"[72]. Assumir uma visão pluralista da juridicidade, reconhecer a existência de Direitos alternativos, não significa emascular o Direito estadual, preconizar a sua irrelevância ou conjeturar a sua desnecessidade, antes, perfilhar a relevância da produção jurídica não estadual que, no que concerne à internet, tem desempenhado um papel crucial e irrefutável.

70 NEVES, A. Castanheira - *Digesta: Escritos acerca do Direito, do Pensamento Jurídico, da sua Metodologia e Outros*. V. I. Coimbra: Coimbra Editora, 1995, p. 27.
71 Desde há anos que aderi à visão de LESSIG, Lawrence - *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999, quando ensina que a regulação se faz através da lei, da norma social, do mercado e da arquitetura.
72 MACHADO, Jónatas E. M. - *Liberdade de Expressão, cit.*, p. 1108

O pluralismo, mais do que uma premissa filosófica, impõe-se com a força das necessidades evidentes para o estudioso da "sociedade da informação e da comunicação"; escrevo com a convicção de que a regulação da rede, obviamente, não dispensa o direito estadual, mas não se esgota no estadualismo. Se queremos mergulhar de modo profícuo na intrincada necessidade de regular os conteúdos disponíveis na rede, temos de reconhecer a existência da *soft law*, perceber que a autorregulação desempenha uma missão insubstituível, reforçar a relevância da regulação contratual (embora sem ignorar que esta está rodeada de riscos, incertezas e abusos), pugnar por um reforço das normas de direito internacional *supra* e *infraestadual*, meditar sobre a regulação através do código e compreender a dimensão fundamental do costume, ainda que sob a designação de *netiqueta*[73], enquanto alicerces vitais para o edifício jurídico que se pretende construir. No contexto específico da internet, encontramo-nos no centro de uma galáxia normativa onde se cruzam estruturas específicas da tecnologia (como a regulação pelo código), do sistema moral (as premissas ciberlibertárias) e do sistema do Direito (porque os Estados foram convocados para solucionar querelas) que importa conciliar.

Como recorda António HESPANHA, "não falta quem defenda que o papel do Estado nos dias de hoje é, mais do que uma regulação directa, o estabelecimento e manutenção de instâncias de meta-observação e avaliação da autorregulação"[74]. Porque o Estado, enquanto regulador, pode recorrer a diferentes armas: *in casu*, o Estado pode servir-se dos prestadores de serviço em rede, enquadrando-os na cruzada do controlo dos conteúdos, através da estatuição do princípio de que estes, em determinadas situações, são responsáveis pelos conteúdos que transmitem; como podem convocar os fornecedores de conteúdos e os proprietários do *hardware* utilizado pelas crianças para a missão de as proteger de conteúdos nefastos; como é preciso consciencializar quem exerce a autoridade parental para o desiderato de proteger os menores, de os sensibilizar para uma navegação segura e impor consequências para o seu inadimplemento. Sem ignorar que a defesa das crianças na rede também se constrói com o contributo da sociedade civil, pela

73 Como eu, REIDENBERG, Joel R. - *Governing Networks and Rule-Making in Cyberspace*. "Emory Law Journal". Georgia. V. 45 (1996), p. 920.
74 HESPANHA, António Manuel - *O Caleidoscópio do Direito: O Direito e a Justiça nos Dias e no Mundo de Hoje. 2.ª Ed., - (o Tempo e a Norma).* Coimbra: Livraria Almedina, 2009, p. 440, em diálogo com LADEUR.

ação, tantas vezes anónima, de pessoas que, no exercício da cidadania ativa, alertam as autoridades para a presença na rede de conteúdos ilegais.

Porque não acompanho a vocação hegemónica do Direito estadual, estou convicto que a proteção, que se procura, exige um compromisso de todos os atores do mundo da internet, porque apenas com um trabalho colaborativo será possível *salvar* as crianças dos conteúdos indesejados, *in casu*, criar um ambiente saudável na rede, para que esta possa corresponder ao sonho dos seus criadores. E, se estou ciente que é impossível purgar da internet todos os conteúdos nocivos às crianças, acredito que é possível uma massiva redução de alguns destes conteúdos, mormente dos conteúdos pedófilos. E sobretudo, podemos tornar mais difícil, muito mais difícil (e mais perigosa) a sua divulgação.

Assim, no que concerne, especificamente, ao caleidoscópio da prevenção das crianças dos conteúdos que navegam na rede, defendo uma construção que apela a diferentes níveis de proteção. Não que tenha tido uma epifania, mas porque, tal como Isaac NEWTON, entendo que para ver mais longe é preciso que nos coloquemos nos ombros dos gigantes[75].

Numa primeira instância, subscrevo que a profícua proteção das crianças tem que centrar-se nelas próprias, dotando-as de *empowerment* que lhes permita desenvencilharem-se das ameaças digitais. Acredito que o caminho mais profícuo para lidar com os problemas decorrentes da utilização da internet constrói-se através da educação; porque, sem educarmos as crianças para os riscos da rede, todo o restante edifício protetor vai ruir. Porque, quando dissecados os mais prementes riscos a que as crianças são [estão?] expostas na rede, percebemos que, numa grande maioria das situações, a criança autocolocou-se em perigo, por ação ou omissão, pelo que, sem a consciencialização das crianças, a batalha será inglória.

75 Pelo que, a construção que trilhei, aproxima-me do pensamento de PALFREY, John/GASSER, Urs - *Born Digital: Understanding the First Generation..., cit.*, p. 11.

Num segundo patamar, é preciso convocar os pais. Porque são estes (bem como os educadores e os pares) a quem incumbe, *prima facie*, consciencializar as crianças sobre os riscos, os perigos, as barreiras legais e culturais, bem como, fornecer as ferramentas tecnológicas e emocionais que as protegem. Como, dos pais, devemos exigir a maturidade para compreender a *cultura de internet das crianças e dos adolescentes* [por estranha que esta possa parecer para os adultos]. Uma compreensão que só poderá advir do diálogo e da negociação. Porque os pais (e restantes educadores, embora primeiro aqueles e apenas depois estes) têm uma missão fundamental: esta defesa intransigente de que os menores devem desenvolver uma consciência crítica, que apenas se desenvolve com uma autonomia construtiva, não significa que os pais fiquem de braços cruzados quando os filhos *brincam na autoestrada*. Por outro lado, não basta convocar os pais para esta missão: é preciso sublinhar que o seu inadimplemento tem consequências jurídicas. Que, da mesma forma que os pais não podem ignorar os perigos a que a criança é exposta no "mundo físico", absterem-se de proteger os filhos na internet, é juridicamente intolerável. Porque é insustentável manter uma construção social que assertivamente abomina os maus-tratos físicos às crianças, mas que tolera as agressões e omissões ao desenvolvimento psicológico, em que se permita que os preconceitos dos adultos sejam impostos às crianças e que a sua liberdade seja coartada arbitrariamente.

Numa terceira instância protetora, defendo a necessidade de apelar para os prestadores de serviço em rede e para os fornecedores de conteúdos, cuja importância é fundamental para construir um ambiente cibernético mais seguro. Faço-o porque, o melhor remédio para proteger as crianças dos conteúdos abjetos que navegam na internet é que estes nunca sejam disponibilizados na *world wide web*. Ou, uma vez colocados na rede, sejam rapidamente removidos. Também por isso, subscrevo uma aceção ampla de fornecedor de conteúdo, que inclui, não apenas o autor, como o administrador do sítio onde a informação foi disponibilizada e ainda aquele que realiza hiperligações conscientes, para concluir que estes são, obviamente, responsáveis civil e criminalmente pelos seus atos. Como, (re)afirmo, os prestadores de serviço em rede podem ser responsabilizados pelo desvalor dos atos de terceiros, se não impedirem o acesso a conteúdos manifestamente ilícitos ou se desrespeitarem decisões administrativas e judiciais. Mas, concomitantemente com as obrigações legais, recai, sobre os fornecedores de conteúdos e prestadores de serviço em rede, a imperatividade moral de pugnarem pela

construção de uma internet mais amiga das crianças. E, quando abdicam desta responsabilidade, legitimam os Estados a intervir.

Finalmente, convoquei os poderes públicos, tendo como premissa a distinção entre os conteúdos ilegais daqueloutros que, apesar de nocivos, são legais. E, se para estes, a primeira resposta não deverá ser do legislador, que apenas deverá regular em *ultima ratio*, para perseguir conteúdos ilegais, enfatizei que a Lei é crucial, seja através de uma regulação direta ou indireta. Porque trago o Estado à colação numa dupla dimensão: numa primeira perspetiva, exige-se legiferação estadual e o exercício da sua *manu militari*, numa ótica repressiva, mas, principalmente, numa ótica preventiva, porquanto, não há nada mais pernicioso para a sã convivência social do que o sentimento de impunidade; mas, também apelei ao Estado, para o exercício de uma regulação indireta, em parceria com outros agentes normogenéticos.

Uma visão panjurídica da sociedade colide com os valores constitucionais da liberdade ao desenvolvimento pessoal. Alguns aspetos da nossa vida são regulados pela Lei; outros não. E esta premissa é válida para a regulação da internet. A compreensão da minha tese exige a destrinça entre os conteúdos ilegais e os conteúdos nocivos, porquanto estes convocam questões de princípio radicalmente diferentes e que exigem respostas jurídicas heterogéneas. Se o combate aos conteúdos ilegais é uma prorrogativa de que os Estados não podem abdicar, a perseguição dos conteúdos nocivos deve, *prima facie*, ser uma incumbência de outros agentes normogenéticos.

Reconheço, assim, a pertinência dos mecanismos de autorregulação, que são parte do património histórico-jurídico da internet, uma necessidade do presente e uma inevitabilidade na regulação futura da rede. Se a tecnologia oferece problemas, também oferece soluções, pelo que a regulação através do código é crucial. Como, através dos contratos, é possível construir uma rede mais segura, em que os princípios e os valores que norteiam a comunidade são defendidos na internet. Como se exige que se respeitem as práticas consuetudinárias que se foram plasmando com o devir da rede. Por outro lado, se algumas condutas na internet provocam externalidades relevantes, outras têm uma eficácia limitada e sem dignidade legal.

O que não significa que os poderes públicos devam abster-se de pugnar contra as informações nocivas para o desenvolvimento integral das crianças; porque a ação jurídica dos Estados não se esgota na criação legislativa e na aplicação de condenações judiciais. Compete ainda aos Estados criar as condições ontológicas para que o Direito alternativo se desenvolva, bem como, deverá ser um agente indutor da transformação da norma social. Porque há sempre duas maneiras de construir uma estrada, os Estados podem optar por regular direta ou indiretamente, sendo que, só devem intervir diretamente, em *ultima ratio*, quando os restantes patamares de proteção falharem ou forem impotentes.

6. CONCLUSÃO

Não tenhamos ilusões de facilitismo: procurar construir um sistema tendente a regular os conteúdos disponíveis na internet que são prejudiciais para as crianças é um *trabalho de Sísifo*. Como é tautológico, é impossível garantir a segurança integral das crianças na internet. Que, por melhor que seja a arquitetura jurídica, que, por mais que se otimize a eidética social, vão persistir comportamentos desviantes na internet que afetam as crianças. Mas o reconhecimento desta inevitabilidade não nos pode acorrentar a preconceitos ciberfóbicos e fazer esquecer que, também fora da internet, a segurança integral inexiste. Porque, se é impossível garantir a proteção integral, é possível mitigar os riscos. E foi essa a minha missão: investigar as premissas que permitem potencializar um ambiente mais favorável às crianças no estranho mundo da internet.

No que separa a ciberfobia da ciberfilia, coloco-me num aristotélico patamar pragmático: porque, se recordei os perigos, fui categórico em afirmar que o maior risco da internet para as crianças é o risco de não usar a internet, porquanto esta é (pode ser!) uma ferramenta fundamental para o seu desenvolvimento integral.

Contrariamente ao pensamento libertário sustento que, se a internet é uma realidade multi-jurídica, não é ajurídica: se é insofismável que a arquitetura da rede e a filosofia dos seus fundadores desafia a regulação estadual, esta é possível, legítima e necessária. Porque, se os novos *media* nos libertaram de limitações espácio-temporais, e o Homem do século XXI é cosmopolita, *sente-se em casa no mundo*[76], vive na globalização, estabelece relações pessoais e patrimoniais numa escala mundial, o *homo electronicus* continua situado num qualquer espaço territorial, sujeito a uma qualquer soberania, com legitimidade para lhe impor comportamentos e punir as suas faltas. Há uma premissa que acompanhou todo o meu raciocínio e esteve abscôndita em cada uma das minhas reflexões, a qual me afasta da doutrina maioritária que centrou a sua atenção na internet: entendo que o ciberespaço não existe! Pelo que, as explicações que procuramos apenas podem ter resposta no mundo físico e um comportamento que é ilícito fora da internet não se converte à legalidade por obra e graça do *ciberespaço*.

Beja, 28 de junho de 2017

76 As palavras são de Hannah ARENDT.

OPINIÃO

UMA CONVERSA COM TITO DE MORAIS [1]

1 Contactos: Site: http://www.MiudosSegurosNa.Net
Facebook: http://www.facebook.com/MiudosSegurosNa.Net
Twitter: http://www.twitter.com/msnn
Google: http://google.com/+ProjectoMiudosSegurosNaNet
LinkedIn: https://www.linkedin.com/company/projecto-miudossegurosna-net

TITO DE MORAIS

Propusemos uma conversa a Tito de Morais. Atendendo à temática, quase em exclusivo, desta edição da «Cyberlawby CIJIC» e à experiência colecionada ao longo dos anos pelo entrevistado, procuramos encontrar uma conversa fluída, consciente, necessária, sobre muitos dos tópicos e problemas que a protecção de crianças e jovens suscitam nesse espaço tão amplo e tão sedutor que a internet hoje representa.

Nuno Teixeira Castro) «***Minimizar riscos. Maximizar benefícios.***»

Comecemos pelo lema do projecto «miudossegurosna.net». Desde o início do projecto até aos dias de hoje, muito caminho foi trilhado. O lema sendo intemporal, mantém a mesma validade?

Tito de Morais) Mantém, se bem que se fosse hoje, substituiria a palavra "riscos" por "danos". Esses é que são de evitar. Os riscos, não tanto. O risco é um motor de desenvolvimento e desde que devidamente ponderado, será positivo. Como diz o ditado, "*quem não arrisca, não petisca*". Até porque, se não corrermos certos riscos dificilmente

aproveitaremos e beneficiaremos das oportunidades que as tecnologias de informação e comunicação nos podem oferecer.

N.T.C.) – (*Ponto de ordem*: ainda que muitas considerações sejam válidas, em moldes semelhantes, para a temática dos *imigrantes digitais*, o foco desta nossa conversa incidirá sobre os *nativos digitais*, i.e., as nossas crianças e jovens.)

A realidade digital assume-se, crescente e diariamente, como uma ferramenta indispensável para os mais diversos e indiferenciados comportamentos humanos. Complementados por uma interacção multiplataforma, este admirável novo mundo, digital rompe com muitos dos cânones tradicionais – pelo menos aqueles que nos terão acompanhado enquanto crescíamos – do crescimento, do ensino, da própria socialização das nossas crianças e jovens. Sendo insofismável que elas serão os adultos do amanhã, estaremos conscientes de tais alterações sociológicas e desse futuro que por eles espera e que lhes legamos?

T.M.) Com quase 20 anos de existência, a distinção entre *nativos digitais e imigrantes digitais* está a morrer[2], pelo que me vejo cada vez menos a usar a expressão. No entanto, tenho dúvidas que os pais e encarregados de educação de hoje, tenham consciência das alterações sociológicas que as tecnologias venham a introduzir no futuro que legam aos seus filhos. Quando falamos de realidade virtual, realidade aumentada, inteligência artificial, é-nos difícil hoje imaginar o impacto que terão num futuro próximo. É-nos difícil hoje imaginar que profissões deixarão de existir e que outras surgirão. Mas esta era também a realidade, se bem que por ventura menos acelerada, da geração que nos precedeu.

N.T.C.) - *O tema carece, evidentemente, de uma visão holística. Insistindo nesta tal de putativa mutação sociológica pressuposta nesse mundo novo digital a explorar, com centenas de interacções meramente virtualizadas, sem contacto humano directo, sem presença de adultos nos diversos processos comunicacionais; sem uma noção e compreensão do valor e proximidade do próximo, do seu semelhante; as noções de liberdade, responsabilidade, limites, riscos, apresentam-se no manto de uma certa confusão a quem, em razão da sua imaturidade natural, convive (mais ou menos) "sozinho" nesta exploração do digital. Este "abandono", "entregue a si próprio", sendo factual, é possível de se contrariar?*

T.M.) É difícil, mas julgo que possível contrariar. A tecnologia tem de ser colocada no seu devido lugar e isso tem de começar desde idade muito tenra. Para tal, é de vital importância pais e encarregados de educação terem disso consciência e não

2 Holton, Doug. The Digital Natives / Digital Immigrants Distinction Is Dead, Or At Least Dying. Consultado em https://edtechdev.wordpress.com/2010/03/19/the-digital-natives-digital-immigrants-distinction-is-dead-or-at-least-dying/ a 04 de Setembro de 2017.

usarem as tecnologias como "ama-seca", como chupeta, como a minha geração fez com o vídeo, por exemplo.

N.T.C.) - *Pois… Penso, também e por exemplo, nos naturais processos de "aceitação" ou "rejeição" grupal. Sendo o ser humano um ser profusamente social, que depende dos outros para se realizar, imaginemos, hipoteticamente, uma ou outra característica pessoal de uma dada criança (ou jovem) – mais ou menos "aceitável" pelo grupo a que quer pertencer. Uma rejeição acarreta um processo de exclusão, social, dessa criança (ou jovem).*
"Entregue a si própria", estarão os pais, a escola, o próprio Estado, capacitados para superar essa, eventual, "exclusão" (ou sentimento de rejeição)?

T.M.) A conformidade social é sem dúvida uma força importante com a qual nos confrontamos ao viver em sociedade. Daí a importância do desenvolvimento do sentido crítico para que os princípios da conformidade social não nos transformem em seres irracionais, submetidos ao coletivo a todo o custo, como se fossemos membros de uma manada. Aí os pais e encarregados de educação, professores e educadores, têm um papel importantíssimo a desempenhar, contribuindo para a afirmação pessoal de cada um, sem contudo, deixarmos de seguir as normas que nos permitem viver em sociedade.

N.T.C.) - *Excelente tópico - A conformidade social. Trago à colação, por exemplo, a dispersão de websites pro-ana[3] pro-mia[4], viajando por redes sociais como o Tumblr, Xanga, LiveJournal, Facebook e o MySpace. Com um dado pendor ideológico, até que ponto é possível contrariar o encapsulamento das crianças e jovens? A pergunta é válida para outras circunstâncias grupais, de proliferação de discurso do ódio, de radicalismos diversos, de procura de extremismos…*
Há instrumentos capazes de actuar nas margens, contrariando os movimentos de radicalização/extremismo digital (mais das vezes seguido de uma concretização no mundo real)?

T.M.) A reflexão é importante. Afinal, houve fenómenos, por exemplo, como o a difusão da doutrina nazi, ou, num passado mais recente, Jim Jones que conduziu à morte cerca de 1000 dos seus seguidores, e ainda não havia Internet. Isto para dizer que, se a Internet é facilitadora da disseminação dos fenómenos que refere, a verdade é que também o é para contrariar esses mesmos fenómenos. Os instrumentos existem, na Internet e fora dela. A questão é se são usados e/ou como são usados.

3 Por exemplo: http://www.myproana.com/
4 Por exemplo: https://missanamia.wordpress.com/tips-pro-mia/

N.T.C.) - *Proponho, por exemplo, uma outra reflexão sobre uma ameaça bem real: o Cyberbullying. Podem, ou melhor, até que ponto saberão os pais, a escola, outros grupos primários, lidar com este fenómeno?*

T.M.) Aí posso responder-lhe claramente que a família, a escola e as comunidades em que estas se inserem não sabem lidar com o *cyberbullying*. Aliás, tal percepção foi o que nos levou - a mim, à Sónia Seixas e ao Luís Fernandes – a escrever o livro "*Cyberbullying – Um guia para pais e educadores*". Curiosamente, nas vésperas do lançamento do livro, o Prof. Daniel Sampaio, autor do prefácio, levou um exemplar ainda em cópias de provas para usar numa série de ações de formação que ia fazer. No final, perguntei-lhe se tinha sido útil, ao que ele me respondeu que tinha sido muito útil e que tinha ajudado a perceber que os adultos estavam muito preocupados com o *bullying* e nada interessados no *cyberbullying*, ao passo que, com os alunos era exatamente o contrário. Esta perceção é, infelizmente, também a que tenho em resultados dos pedidos de ajuda que nos chegam por diversos meios.

N.T.C.) *A propósito. Recupero um trecho, ainda que radicalmente mediatizado e explorado, o jogo «Baleia azul». Isto suscita-me logo uma questão. Os curadores de tal "jogo" conseguiam identificar, de forma mais ou menos fácil, muitas das nossas crianças, admitamos, mais fragilizadas. Algumas destas vítimas, conseguiram surpreender – quer pela gravidade dos actos cometidos sobre elas mesmas, quer pela forma como se deixaram seduzir a tal práctica – os seus respectivos pais (em sentido lato). Esta ameaça viajou, em modo silente e quasi-anónimo, até às vítimas. Podem os pais, muitos deles autênticos analfabetos digitais, proteger as suas crianças e jovens, no imediato, delas próprias?*

T.M.) Podem. O tipo de problemas que refere, tal como, por exemplo, a anorexia, a bulimia, a radicalização, etc. não são um problema tecnológico, mas um problema relacionado com a saúde mental e com o bem-estar das crianças e dos jovens. Um uso abusivo das tecnologias poderá agravar tal condição. Se pais e encarregados de educação, família, escola e comunidade estiverem atentos, o analfabetismo digital poderá não ser um problema. A dificuldade, invariavelmente, surge da junção dos dois: do analfabetismo parental e do analfabetismo digital. Dito isto, importa, ainda, ter bem presente que situações haverá em que mesmo filhos de pais atentos e digitalmente cultos, podem ser aliciados e vitimizados. Afinal, não estamos perante autómatos juvenis, mas de seres com vontade própria.

N.T.C.) - *Desligar o cabo de rede ou o wifi em casa é sempre uma solução "imediatista". Não sendo "salomónica", poderá obstar a uma conexão digital em casa. Porém o contacto com o mundo digital estabelece-se por multiplataforma. É o telemóvel (smartphone, tablet, phablet, …) que a criança leva para a escola para poder contactar os pais, que, além disso, tem a porta aberta para um acesso à internet; é a sala de estudo da escola que tem um pc com acesso à internet; é o café em frente à escola que dispõem de um pc com acesso à net;… A "internet em qualquer lugar, a qualquer hora" é uma*

realidade que se nos impõe diariamente. Como podem os pais, mais ou menos imigrantes, alfabetizados ou não, digitais, terem algum controlo, alguma segurança, ante um cardápio tão completo de "riscos"?

T.M.) Sou de opinião que parte do problema é pensarmos mais em termos de controlo e não tanto de acompanhamento e autonomia. O controlo é importante sobretudo na primeira infância, mas o acompanhamento e a educação para a autonomia são essenciais, no meu ponto de vista. Resumindo, julgo que é um processo que começa por ser de controlo, passa a ser de acompanhamento para se tornar mais tarde num processo de "*condução autónoma*". Durante essa evolução, aos pais compete educar os filhos para que tomem as decisões corretas no futuro, mesmo sem nunca conseguir garantir que tal acontecerá. De outra forma, se o processo se resumir só ao controlo, dificilmente criaremos cidadãos autónomos e responsáveis.

N.T.C.) – *Educação. Sem dúvida um tema sempre aliciante. Por exemplo, uma educação digital, trilhando uma consolidação, desejável, de um incremento da literacia digital, permitiria mitigar muitos destes "riscos". Além dos anúncios, recentes, de um Plano Nacional de Leitura 2027, com uma aposta na literacia científica e digital*[5]*; de uma Iniciativa Nacional Competências Digitais e.2030 - INCoDe.2030* [6]*, com uma aposta clara na inclusão e capacitação digitais; neste conspecto, em concreto, no dia a dia de convivência com crianças, jovens, pais, escola, psicólogos, o que tem notado como "lacunas" a colmatar?*

T.M.) Acho ambas as iniciativas excelentes. As principais lacunas a colmatar:

- Tirando uma ou outra exceção, a utilização ética, responsável e segura das tecnologias de informação e comunicação não faz parte dos curricula escolares
- A segurança da informação é focada sobretudo como uma questão tecnológica, ignorando a generalidade das vezes a componente "pessoas", o elo mais fraco da segurança.

N.T.C.) – *Europeízando. Sobre o Regulamento Geral de Protecção de dados*[7]*. Um tema a abordar com outra profundidade já no início do próximo ano lectivo, o Artigo 8.º, n.º1, in fine*[8] *do RGPD. Uma vez que o legislador europeu assentiu na liberdade de*

5 Por exemplo: http://www.portugal.gov.pt/pt/ministerios/medu/noticias/20170330-medu-pnl-2027.aspx
6Por exemplo: http://www.tsf.pt/politica/interior/costa-quer-aposta-nas-competencias-digitais-para-mudar-paradigma-economico-5767588.html
7 Disponível em:
http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT
8 « *Artigo 8.o - Condições aplicáveis ao consentimento de crianças em relação aos serviços da sociedade da informação*

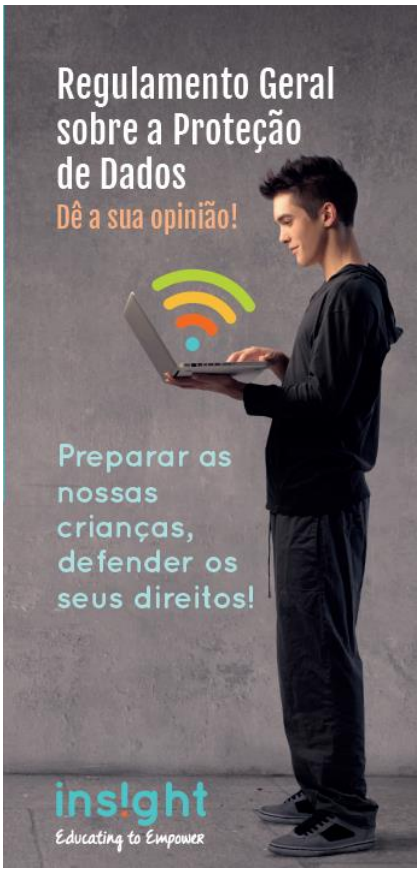
1. *Quando for aplicável o artigo 6.o, n.o 1, alínea a), no que respeita à oferta direta de serviços da sociedade da informação às crianças, dos dados pessoais de crianças é lícito se elas tiverem pelo menos 16 anos. Caso a criança tenha menos de 16 anos, o tratamento só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança.*

interpretação desta parte final a cada Estado-membro, antes que o legislador nacional se pronuncie em razão da idade a observar, será inevitável auscultar a sociedade civil, no seu todo, incluindo os principais visados pela temática – as nossas crianças e jovens. Conheço algumas das iniciativas que, patrocinadas pelo GDPR working group, o Tito de Morais quer introduzir a debate em Portugal. Pode falar-nos um pouco sobre isto?

T.M.) O RGPD tem sido muito falado ao longo do último ano, mas pouco se tem falado do seu artigo 8º, um dos poucos que concede algum espaço de manobra aos países da EU. A génese da redação final do artigo 8º foi, no meu ponto de vista, um processo muito pouco transparente e contra o qual me manifestei[9] perante um silêncio ensurdecedor que à época se verificou não só em Portugal, mas também noutros países da EU. Na altura associei-me a outras pessoas e organizações a nível europeu, procurando levar a uma reflexão antes da aprovação do RGPD pelo Parlamento Europeu. Não tendo resultado tal iniciativa e percebendo que o tema do consentimento parental não estava a ser colocado na agenda do debate público, já este ano, começámos a trabalhar numa nova iniciativa no sentido de lançarmos o debate público sobre o tema, bem como uma consulta aos principais visados: os jovens. Assim, nasce a iniciativa #GDPRHaveYourSay , no âmbito da qual publicámos uma brochura com 10 razões pelas quais os adolescentes não precisam de consentimento parental para aceder aos serviços da sociedade de informação e no âmbito da qual agora em Setembro iremos lançar um Manual de Ação Para Jovens. Tal permitirá ouvir os jovens europeus sobre os seus direitos em geral e sobre o consentimento parental em particular. Os potenciais interessados em aderir a esta iniciativa podem contatar-nos em https://www.facebook.com/GDPRhaveyoursay/.

Os Estados-Membros podem dispor no seu direito uma idade inferior para os efeitos referidos, desde que essa idade não seja inferior a 13 anos.»

9 Morais, Tito de. Opinião: Idade Mínima de 16 Anos Para Usar a Internet?! Consultado em 04 de Setembro de 2017 em http://tek.sapo.pt/opiniao/artigos/opiniao-idade-minima-de-16-anos-para-usar-a-internet



N.T.C.) - *Neste sentido, aproveito esta ocasião para anunciar, em primeira mão, que quer o CIJIC – Centro de investigação jurídica do ciberespaço – da Faculdade de direito da Universidade de Lisboa; quer o Capítulo português da ISOC; ambos demonstraram a respectiva disponibilidade para participarem activamente na futura discussão(ões) pública(s) sobre o tema. Quer na fase intermédia, quer posteriormente na sessão de avaliação final no dia europeu de protecção de dados, em 2018.*

T.M.) Se percebi bem, o CIJIC e o ISOC.PT aderem à iniciativa #RGPDDáATuaOpinião, o que quer dizer que autorizam a inclusão dos respetivos logotipos na brochura e no Manual de Ação Para Jovens e que nos ajudarão na divulgação dos mesmos? A ser assim, são boas notícias!

N.T.C.) *Não obstante, em consciência, e por comparação entre o começo do miudossegurosnanet e o hoje, a participação activa nestes temas terá evoluído como o desejado? Ou apresenta-se demarcada, quase sempre, por uma meia-dúzia de (mesmas) pessoas. Partilha desta ideia da falta de uma maior mobilização da sociedade civil?*

T.M.) Não concordo inteiramente com essa ideia. De facto, se recuarmos a 2003, ano da criação do Projeto MiudosSegurosNa.Net, este não era um tema, não havia recursos em língua Portuguesa, não havia especialistas. Era, digamos, um não-tema. Inexistente, como, de uma ou outra forma, ainda o é na agenda pública. Na prática, a

realidade já é um pouco diferente, tendo-se transformado um pouco num tema pejado de *treinadores de bancada* repleto de palpites para fornecer a quem os queira ouvir.

A crítica que sugere é outra. De facto, seja neste tema, seja noutros, a sociedade civil Portuguesa é muito pouco interventiva, sobretudo no que diz respeito a políticas públicas. Assiste-se a uma realidade preocupante que é a dependência excessiva financeira das organizações da sociedade civil dos apoios e subsídios estatais, levando a que muitas ONG sejam silenciosas relativamente a políticas governamentais. Neste caso, a situação agrava-se por muitas delas não disporem de *know-how* no domínio tecnológico que lhes permita conhecer as situações em profundidade e intervir publicamente sobre as mesmas.

N.T.C.) – *Para finalizar a nossa conversa, que já vai longa, um desafio à antecipação do que poderá ser um pouco o "futuro"sobre a protecção de crianças e jovens, o que espera deste nos próximos anos?*

T.M.) O futuro define-se hoje e antevejo aplicações abusivas da Inteligência Artificial e da Internet das Coisas, nomeadamente ao nível dos *SmartToys*. Já ao nível do que gostaria de ver, seria excelente que assistíssemos a uma maior participação cívica dos jovens, lutando e fazendo valer os seus direitos *online*, para que o discurso da segurança das crianças e dos jovens não continue a ser um discurso dominado pelos adultos e deslocado da realidade, a exemplo do, aludido, artigo 8.º do RGPD.

Setembro de 2017

CYBERLAW
by CIJIC

EDUCAÇÃO DIGITAL: *ENTRE NATIVOS E IMIGRANTES DIGITAIS*

MARCELO CRESPO [1]

1 Endereço de correio electrónico: marcelocrespo@peckadvogados.com.br

Educação digital – ensino – sociedade digital – nativos digitais – imigrantes digitais

Digital education – education – digital society – digital natives – digital immigrants

Temos presenciado grandes mudanças sociais derivadas do crescente avanço tecnológico, que tem tornado a vida das pessoas cada vez mais digitais. Com novas formas de comunicação revolucionando o mundo, é extremamente fácil o acesso a conteúdos diversos, o que pode favorecer o processo de aprendizagem e, assim, a educação.

Esse contexto digital permitiu a criação do meio ambiente digital, que é o espaço de comunicação aberto e que interconecta computadores e pessoas. Quando há conexão entre computador e meio ambiente digital é que se poderá falar em cultura digital, que envolve a propagação de informações do que fora criado até então.

Estas inovações alteram o modo de pensar e de agir da sociedade, resultando em transformações na área educacional, as vezes melhorando, as vezes piorando o contexto de ensino. É que há inegável facilitação no aprendizado, alcançando desde o ensino mais fundamental até o mais avançado. Por outro lado, muitas oportunidades são desperdiçadas pelo mau uso da tecnologia quando se deixa de aproveita-la adequadamente.

Não se pode negar, porém, que o contexto de propagação e universalização da informação auxilia crianças e adolescentes a absorverem conteúdos dos mais variados, o que tem gerado mutações no meio ambiente escolar. Surgem, assim, os nativos digitais e os imigrantes digitais[1].

É que os alunos atuais já cresceram com tecnologia e passaram a vida cercada por ela, provavelmente com mais tempo gasto perante a TV, internet e videogames que lendo livros. Estes alunos funcionam melhor quando conectados à tecnologia e em redes e quando recebem

recompensas frequentes. Os demais, os mais antigos, adotaram alguns aspectos da tecnologia, mas ainda têm um certo "sotaque"[2].

Assim, nativos digitais são verdadeiras personalidades conectadas, que pensam de maneira hipertextual e que encontram vários ambientes de conexão para a troca de informações e desenvolvimento de suas competências.

A tecnologia, assim, propicia mudanças no processo cognitivo da geração atual, requerendo maior rapidez para a execução de determinados comandos. Há, assim, verdadeira divisão na conjuntura cultural no que diz respeito à tecnologia, havendo dois grandes grupos: os nativos e os imigrantes digitais.

Os aspectos tecnológicos favorecem um melhor aproveitamento do processamento de informações dos nativos digitais, de modo que os jovens atuais buscam interatividade também em sala de aula já que suas bases se fundam em constantes inovações e na evolução dos aparatos tecnológicos. Isso, naturalmente, leva a um impasse entre gerações, que vê nos docentes imigrantes digitais que precisam buscar novos métodos de transmissão de conhecimentos ligados às tecnologias.

Este cenário é representativo de uma incomunicabilidade entre os sujeitos escolares já que da parte dos professores diz-se que os jovens se mostram apáticos, indisciplinados e desinteressados e, da parte dos alunos diz-se que os docentes são despreparados e sem didática. Somente uma evolução nos estabelecimentos de ensino podem mudar isso, sendo imprescindível que os professores estejam inseridos no campo tecnológico, com conhecimento suficiente para atuar com equipamentos e ferramentas que possam intermediar conhecimento em nível satisfatório para ambos.

Há alguns anos bastava que o professor pudesse transmitir aos alunos o que constava dos livros. Mas, com o avanço tecnológico exige-se mais que isso. Cabe a eles se envolverem em novos temas e contextos com os quais os alunos possam se deparar com diversas facetas proporcionadas

em formatos multimídia que os discentes poderão alcançar o conhecimento pretendido por meio de textos, sons e interatividade.

É característico dos nativos digitais que se apeguem a modelos hipermídia, o que se verifica facilmente pelos seus pensamentos não lineares. Eles recebem informações de forma randômica, rápida e preferem gráficos a textos.

O uso de tecnologia no ensino atual é imprescindível, não bastando que as aulas sejam mais dinâmicas. Ocorre que muitos docentes ainda são muito resistentes quanto a se envolverem com tecnologia em sala de aula e não estão devidamente capacitados para lidar com a variedade tecnológica, faltando-lhes, muitas vezes, oferta de treinamentos e capacitação.

A internet não é mais um extraordinário ferramental, mas uma plataforma mínima para a exploração do conhecimento que deverá estar conectada a redes sociais, causadoras de mudanças culturais importantes e configurando, até mesmo, um novo meio didático.

E o desafio é grande porque os docentes também precisam estar preparados para promover a inclusão digital dos que não têm acesso à tecnologia. A responsabilidade do professor é ainda maior, com isso. E essas mudanças não ocorrem por mera coincidência ou por convenção social, mas pela necessidade de mudanças qualitativas nos processos de aprendizagem.

Quando se fala em transformação do papel do professor, não se trata, portanto, de mera incorporação da tecnologia ao seu dia-a-dia docente. Sua figura deixa de ser um transmissor absoluto para se tornar um facilitador de descobertas já que a plateia não é mais simplesmente receptora. O docente deveria, assim, ser um treinador, um guia e não apenas um repetidor/transmissor.

Não se deve estranhar, portanto, que nativos e imigrantes digitais vivam em choque cultural.

Mas, então, qual a solução?

Não é crível que os nativos digitais regredirão, sendo isto bastante para que se tenha a certeza de que dependerá dos imigrantes digitais o aprendizado sobre novas tecnologias e metodologias. Os professores atuais devem se adaptar para que possam falar em linguagem o quanto mais semelhante possível à dos estudantes, isto é, mais rápido, mais randômico e multimídia. Prensky fala em conteúdos "legado" (ler, escrever, raciocínio lógico, etc) e "futuro" (software, hardware, robótica, nanotecnologia, genoma, etc)[3].

Somente uma adaptação neste sentido permitirá um desejável equilíbrio entre o ensinar e o aprender.

---

1 https://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf, acesso em 14.08.2017.
2 *Idem.*
3 *Ibidem*..