COLEÇÃO FORMAÇÃO CONTÍNUA

A INTERNET E AS CRIANÇAS

RISCOS E POTENCIALIDADES

JURISDIÇÃO DA FAMÍLIA E DAS CRIANÇAS

JULHO 2018

CENTRO DE ESTUDOS JUDICIÁRIOS

Diretor do CEJ
João Manuel da Silva Miguel, Juiz Conselheiro

Diretores Adjuntos
Paulo Alexandre Pereira Guerra, Juiz Desembargador
Luís Manuel Cunha Silva Pereira, Procurador-Geral Adjunto

Coordenador do Departamento da Formação
Edgar Taborda Lopes, Juiz Desembargador

Coordenadora do Departamento de Relações Internacionais
Helena Leitão, Procuradora da República

Grafismo
Ana Caçapo - CEJ

Capa
Edifício do CEJ

Foto
Victor Pimenta - CEJ

A internet em geral e as redes sociais vieram colocar novos desafios ao exercício das responsabilidades parentais, quer pela facilidade de acesso, quer pelo difícil controlo da segurança.

A redobrada atenção que a todos se exige implica conhecimento e reflexão sobre o que pode estar em causa.

O Centro de Estudos Judiciários, através das acções de formação organizadas pela sua Jurisdição da Família e das Crianças, tem procurado contribuir para esse debate.

O resultado é espelhado em mais este e-book da "Coleção Formação Contínua".

(ETL)

CENTRO
DE ESTUDOS
JUDICIÁRIOS

Ficha Técnica

Nome:

A Internet e as crianças – riscos e potencialidades

Jurisdição da Família e das Crianças:

Ana Maria Carvalho Massena Carreiro (Procuradora da República, Docente do CEJ e Coordenadora da Jurisdição)
Maria Gomes Bernardo Perquilhas (Juíza de Direito e Docente do CEJ)
Ana Teresa Pinto Leal (Procuradora da República e Docente do CEJ)
Chandra Gracias (Juíza de Direito e Docente do CEJ)
José Eduardo Gonçalves Barbosa Lima (Procurador da República e Docente do CEJ)

Coleção:

Formação Contínua

Plano de Formação 2015/2016:

Temas de Direito da Família e das Crianças – 6, 13, 20 e 27 de maio de 2016 (programa)

Conceção e organização:

Jurisdição da Família e das Crianças

Intervenientes:

Manuel Magriço – Procurador da República na Secção de Família e Menores da Amadora da comarca de Lisboa Oeste
José Alberto Simões – Docente universitário da Universidade Nova de Lisboa
Ivone Patrão – Psicóloga clínica, ISPA
Tito de Morais – Fundador de "MiudosSegurosNa.Net" e editor da única newsletter portuguesa sobre a segurança online de crianças e jovens

Revisão final:

Edgar Taborda Lopes – Juiz Desembargador, Coordenador do Departamento da Formação do CEJ
Ana Caçapo – Departamento da Formação do CEJ
Lucília do Carmo – Departamento da Formação do CEJ

Notas:

Para a visualização correta dos e-books recomenda-se o seu descarregamento e a utilização do programa Adobe Acrobat Reader.

Foi respeitada a opção dos autores na utilização ou não do novo Acordo Ortográfico.

Os conteúdos e textos constantes desta obra, bem como as opiniões pessoais aqui expressas, são da exclusiva responsabilidade dos/as seus/suas Autores/as não vinculando nem necessariamente correspondendo à posição do Centro de Estudos Judiciários relativamente às temáticas abordadas.

A reprodução total ou parcial dos seus conteúdos e textos está autorizada sempre que seja devidamente citada a respetiva origem.

Forma de citação de um livro eletrónico (NP405-4):

AUTOR(ES) – **Título** [Em linha]. a ed. Edição. Local de edição: Editor, ano de edição.
[Consult. Data de consulta]. Disponível na internet: <URL:>. ISBN.

Exemplo:
Direito Bancário [Em linha]. Lisboa: Centro de Estudos Judiciários, 2015.
[Consult. 12 mar. 2015].
Disponível na
internet: <URL: http://www.cej.mj.pt/cej/recursos/ebooks/civil/Direito_Bancario.pdf.
ISBN 978-972-9122-98-9.

Registo das revisões efetuadas ao e-book

Identificação da versão	Data de atualização
1.ª edição –25/07/2018	

A Internet e as crianças – riscos e potencialidades

Índice

CENTRO
DE ESTUDOS
JUDICIÁRIOS

1.

A Internet e as crianças – riscos e potencialidades

Manuel Magriço

CENTRO
DE ESTUDOS
JUDICIÁRIOS

A INTERNET E AS CRIANÇAS – RISCOS E POTENCIALIDADES

Manuel Magriço*

I. Introdução

1.1. Considerações iniciais

O contínuo e rápido desenvolvimento das Tecnologias de Informação e Comunicação (TIC) fez com que os Sistemas de Informação (SI) sejam hoje parte integrante da vida das pessoas, das empresas, dos governos e das organizações internacionais. A *"sociedade do papel"* tem transitado de uma forma acelerada para uma *"sociedade digital",* afluindo na Era da Informação.

Em termos similares, no que concerne a práticas delituosas de natureza criminal, temos assistido a uma transferência das ações criminosas para o Ciberespaço com a utilização intensiva das TIC e dos SI.

A presente análise incide brevemente sobre riscos e potencialidades da Internet para as crianças e para os mais jovens e corresponde a uma comunicação efetuada no Centro de Estudos Judiciários, no dia 13 de Maio de 2016, no âmbito do círculo de formação dedicado a «Temas de Direito da Família e das Crianças» [1]. Abordam-se as inúmeras variáveis e transmutações que este *locus* encerra, com destaque para as decorrências da introdução em curtos intervalos de tempo de novas tecnologias e serviços e sem escamotear a especificidade da população alvo, os mais jovens.

O sistema legal tem produzido inúmeros textos normativos, no âmbito da Investigação Criminal (IC) que manifestam preocupação com as atividades criminosas no Ciberespaço, designadamente no que concerne ao abuso sexual de crianças e a pornografia de menores e de que são exemplo, entre outros, o Código Penal (CP), a Lei do Cibercrime (LCiber), a

*Procurador da República na Secção de Família e Menores da Amadora da comarca de Lisboa Oeste.
[1] Seguindo-se parcialmente o escrito em MAGRIÇO, Manuel Eduardo Aires Magriço – A **Exploração Sexual de Crianças no Ciberespaço**, 2014, Lisboa, Aletheia Editores- ISBN – 9789896226640.

Convenção do Conselho da Europa contra a Exploração e o Abuso Sexual de Crianças e a Diretiva do Parlamento Europeu relativa à luta contra o Abuso e a Exploração Sexual de Crianças e a Pornografia Infantil, esta última, de 13 de dezembro de 2011.

Tem-se presente que as crianças e os mais jovens sentem grande atratividade pelas novas tecnologias, pelo que a análise deste tema que tem como sujeitos seres humanos nos primórdios da sua formação emocional, salvaguarda do futuro da sociedade, impõe que a abordagem seja realizada com enorme delicadeza e se lhe reconheça primordial importância, sobretudo na área da Família e das Crianças.

1.2. Casos de referência a nível internacional

Caso *Cathedral*

Um dos processos-crime que maior impacto teve na comunicação social ocorreu nos E.U.A. – Estados Unidos da América e é identificado como o caso *Cathedral* iniciado no Estado da Califórnia, em abril de 1996 (Leite, 2004, p. 15 e 16). As investigações tiveram origem num pequeno episódio que à partida parecia isolado, mas que acabou por envolver várias centenas de investigadores, de vários países, face a um número incalculável de vítimas. A história do processo judicial inicia-se com a visita de uma criança de 10 anos a casa de uma amiga da escola, para aí passar o fim de semana. Durante essa visita, o pai da amiga fechou a criança no seu quarto, onde se encontrava um computador ligado à Internet equipado com uma *webcam*. No seu quarto, o pai da amiga abusou sexualmente da criança, tendo filmado os abusos e difundido os mesmos, em tempo real, para o Ciberespaço, através da referida câmara de filmar. Durante o abuso sexual, o agressor recebeu instruções das pessoas que estavam a assistir pela Internet, relativamente aos abusos sexuais que deveriam ser praticados com a criança. As imagens foram difundidas num *website*, denominado *Orchid Club*. O agressor gravou as imagens do ato que praticou e vendeu-as, a troco de quantias monetárias, através da Internet. A investigação descobriu o que sucedeu através do testemunho da criança em causa e o agressor foi condenado a 100 anos de prisão.

Caso *Wonderworld*

Após a análise efetuada ao computador do agressor do caso *Cathedral* foram descobertas ligações relativas a outros clubes, que se dedicavam à prática de atos da mesma natureza, entre eles o *Wonderland Club*. Esse clube era altamente organizado, constituído por um presidente, um secretário e um comité executivo, existindo regras estritas de admissão e expulsão de membros. O acesso ao clube era também muito limitado, existindo cinco graus de segurança e várias áreas com códigos e informação encriptadas. Muita desta informação ou áreas do clube nunca foram descodificadas com sucesso pela investigação e por isso ficarão desconhecidas para sempre. Entre os dados que a investigação criminal conseguiu obter, encontravam-se 1.263 crianças diferentes, num total de 750 mil imagens e 1.800 horas de filme.

À semelhança do caso *Cathedral*, os membros do *Wonderland Club* abusavam de crianças com difusão de imagens em tempo real, seguindo instruções dos outros membros em linha. O membro mais ativo desse clube, que mantinha várias crianças detidas em casa, foi condenado numa pena de 12 anos de prisão.

Na sequência deste caso, detetaram-se conexões a vários países Europeus, tendo sido efetuadas buscas, apreensões e detenções de pessoas, de forma simultânea, nos seguintes países: Austrália, Áustria, Bélgica, Finlândia, França, Alemanha, Itália, Noruega, Portugal, E.U.A., Inglaterra e Suécia.

Operação *Avalanche*

A Operação *Avalanche* teve início nos E.U.A. em 1999 depois de terem sido apresentadas cerca de 250 queixas por parte de utilizadores da Internet por todo o mundo. As queixas referiam-se à maior rede de exploração sexual de crianças ativa, à data, nos E.U.A., denominada *Landslile Productions*. Tratava-se de um Portal contendo imagens de pornografia de menores, com ligações a aproximadamente 300 páginas de Internet, os quais continham também material de pornografia de menores. O acesso a essas imagens e vídeos de crianças era concretizado mediante pagamentos efetuados através de cartões de crédito. Estimou-se que este sítio tivesse cerca de 250.000 subscritores. Um mês de subscrição tinha um custo de 30 dólares. Em apenas 1 mês, o *website* em referência gerou um lucro US$ 1.400.000,00. A associação criminosa encontrava-se sediada nos E.U.A., tinham 1 parceiro na Rússia e 4 na Indonésia (Ecpat, 2011, p. 154).

Cerca de 100 pessoas foram acusadas pela prática de crimes contra a infância nos E.U.A., designadamente por posse e disseminação de pornografia de menores. Os suspeitos foram localizados através dos dados dos pagamentos efetuados com os cartões de crédito. O líder da associação criminosa, que se encontrava a gerir o Portal foi condenado a 1.335 anos de prisão. A mulher, que tratava da contabilidade do Portal, foi condenada a 14 anos de prisão.

O *FBI – Federal Bureau of Investigation* forneceu às Autoridades Inglesas informação sobre 7.272 suspeitos residentes noutros países. No total, a Polícia Inglesa concretizou 3.744 detenções durante a investigação da "Operação *Avalanche*" que em território Britânico foi denominada "Operação *Ore*". Foram acusados 1.848 suspeitos dos quais foram condenados 1.451.

Os parágrafos seguintes constituem registo dos aspetos mais relevantes que emergem da revisão dos casos acima descritos, e permitem distinguir papéis entre diferentes intervenientes, no âmbito da exploração sexual de crianças:

- Atores – os que aparecem nas imagens como abusadores;

- Produtores e realizadores – os que contribuem para a captação de imagem e produção do material pornográfico, diretamente ou fornecendo meios técnicos ou financeiros;

- Distribuidores – os que entram em contacto apenas com o produto final e o promovem e fornecem aos destinatários; e por fim,

- Consumidores.

A distinção supra releva de diferentes tipos de atividade com um denominador comum, toda ela de índole criminal e com utilização do Ciberespaço e das TI. Os locais de ocorrência dessas atividades são de difícil determinação e contabilização.

É difícil estimar o número de *websites* a nível mundial que retratam imagens de abuso infantil. A *Internet Watch Foundation* (IWF) identificou e tomou medidas contra 16.700 casos de conteúdos de pornografia de menores em páginas da *web*, em todo o mundo em 2010, em comparação com a identificação de cerca de 10.656 em 2006 (IWF, 2007-2010, p. 8). No entanto, a IWF reconhece a dificuldade de comparar dados anuais. As rápidas mudanças no armazenamento e manipulação de imagens de abuso infantil tornam o número de dados de imagens e páginas *web* incompatíveis, o que dificulta a comparação de dados.

O aumento de casos, observado entre 2006 e 2010, pode ser atribuído a uma mudança nos padrões do armazenamento das imagens – em vez de se colocar coleções de imagens numa pasta, ou numa única página da *web*, o conteúdo pode estar a ser disponibilizado em vários *websites*. Contudo, é de realçar que as imagens de abuso sexual de crianças são cada vez mais comuns entre as redes de indivíduos ligados através das redes *peer-to-peer* (P2P)[2] de distribuição e esse *modus operandi* não necessita de armazenamento das imagens em sistemas propriedade de terceiros (i.e. fornecedores de serviços de Internet – ISP). Há milhões de imagens de abuso de menores na Internet, com dezenas de milhares de crianças retratadas em imagens individuais, relacionadas com o abuso sexual de crianças (Carr et al., 2009, p. 29). Uma vez na Internet, as imagens podem ser facilmente transmitidas para outros *websites*, carregadas para telemóveis ou distribuídas a um número desconhecido de destinatários via *e-mail* de um modo semelhante à difusão de um vírus informático, sem o conhecimento ou consentimento da pessoa retratada. Potenciais agressores são capazes de comunicar e partilhar imagens e outros materiais em todo o mundo. Conexões de alta velocidade à Internet, maior largura de banda, aumento do uso de redes P2P, mecanismos de compressão de dados, tecnologia mais sofisticada, técnicas de criptografia para facilitar a distribuição anónima, e novos meios de acesso à Internet através de Wi-Fi em telemóveis e com cartões pré-pagos, tudo isto reduz a rastreabilidade de quem utiliza esses meios e contribui para o aumento da atividade de exploração abusiva e *on-line* de crianças. A criança não tem controlo sobre as imagens e estas podem permanecer para sempre no ciberespaço. Algumas imagens atualmente em circulação podem ter sido produzidas há mais de 20 ou 30 anos e desde então foram digitalizadas e depois publicadas na Internet. No entanto, a grande maioria das imagens no ciberespaço foi produzida mais recentemente e estão ligadas à disponibilização de novas tecnologias de alta qualidade, designadamente câmaras digitais, e à circunstância da Internet ser hoje um produto de

[2] Peer-to-peer (P2P) - *software* que permite transmissão de dados diretamente de um computador para outro através da Internet, sem a necessidade de envolver um servidor de terceiros.

consumo em massa. Estas imagens mais recentes podem ter origem no ambiente familiar da criança, no seu círculo social, ou ter sido adquiridas através da prostituição infantil de menores.

A colocação de imagens de abuso infantil em linha pode ter consequências duradouras para as crianças. Essas imagens, uma vez publicadas no ciberespaço, são quase impossíveis de eliminar. As crianças dessas fotos podem dar-se conta que, para o resto de suas vidas, alguém pode estar a visualizar as suas fotografias na Internet. Por outro lado, a ameaça da publicação das imagens pode, por si só, constituir uma forma de coação, utilizada por abusadores sexuais de crianças, permitindo-lhes continuar o abuso sexual a longo prazo.

Os agressores também *"vendem"* as crianças para fins de abuso sexual, em linha em tempo real. Para o efeito, os utilizadores publicitam na sua *peer* (rede privada) *on-line* a sua intenção de abusar de uma criança numa data/hora (Tink et al., p. 10-14). Aqueles que desejam assistir ao vivo ao abuso organizam-se com o agressor para estar em linha naquele momento. O pagamento para assistir a este ato criminoso pode ser efetuado em dinheiro ou através da contraprestação de imagens ou produtos estupefacientes. As crianças podem ser atraídas para a casa do ator, e a vítima do abuso sexual, pode ou não estar ciente de que a transmissão ao vivo está a ocorrer.

1.3. Uma em Cinco

Segundo dados disponíveis do Conselho da Europa, cerca de uma criança em cinco na Europa é vítima de alguma forma de violência sexual (Lalor et al.). A violência sexual pode assumir muitas formas, tais como o incesto, pornografia, prostituição, tráfico de seres humanos, aliciamento pela internet, exploração sexual e abuso sexual. Todas elas podem causar, e causam, graves danos à saúde mental e física das crianças. As consequências do abuso sexual prolongam-se até à vida adulta das crianças – os seus testemunhos na primeira pessoa mostram que a tristeza e a dor continuam a acompanhá-las secretamente ao longo de toda a sua vida.

Impõe-se, pelos motivos acima elencados, que os diversos Estados, as famílias, os operadores judiciários e a sociedade civil em geral adotem uma atitude proativa em vista à proteção dos mais jovens contra este tipo de práticas em ordem a:

a) Prevenir e combater a exploração sexual e o abuso sexual;

b) Proteger os direitos das crianças vítimas de violência sexual;

c) Terminar com a impunidade dos perpetradores de violência sexual através da harmonização do direito penal; e

d) Promover a cooperação nacional e internacional contra a exploração sexual e o abuso sexual de crianças.

II. Exploração Sexual de Crianças: Um Negócio Mundial

O compromisso e os esforços de muitos atores da comunidade internacional, autoridades públicas, ONG´S, do setor privado, designadamente os ISP e do setor de telecomunicações e das empresas emissoras de cartões de crédito, entre outros, conduziram à aplicação de muitas medidas efetivas, tendentes à eliminação da exploração sexual de crianças no Ciberespaço, exemplificando-se as seguintes:

a) Reformas legislativas;

b) Desmantelamento de redes de comercialização de material de abuso sexual de menores;

c) Relatórios com recomendações dirigidas aos utilizadores da Internet;

d) Limitações no acesso e bloqueio de *sites* da Internet;

e) Apreensões de material de abuso sexual de menores, prisões de predadores sexuais, campanhas de sensibilização, desenvolvimento de *software* de controlo parental, entre outras iniciativas.

No entanto, apesar destas iniciativas, múltiplas e variadas, a distribuição de material de abuso sexual de menores na Internet, persiste como um negócio muito lucrativo, com um valor de mercado estimado em milhares de milhões de dólares americanos. O fácil acesso às novas tecnologias, as constantes alterações nos métodos de produção e padrões de consumo, a que acresce a dimensão internacional da distribuição de material de abuso sexual de crianças, dificultam a luta contra este flagelo.

O número de *website*s dedicados à pornografia infantil está em crescimento constante em todo o mundo. Entre 2001 e 2004 o número de *sites* cresceu quase 50%. Em 2004 foram identificados 480.000 *sites* relacionados com este fenómeno. O número de predadores de crianças, ligados à Internet em qualquer momento, é estimado em 750.000.

Em 2009, o Centro Nacional de Crianças Exploradas e Desaparecidas (NCMEC), dos Estados Unidos da América, concluiu que, de um total de 681.275 *websites* analisados, foram localizados 592.044 *website*s com material de abuso sexual de menores.

Em 2007, a IWF no Reino Unido recebeu 3.487 relatórios de locais no Ciberespaço com material de abuso infantil, incluindo 2.755 domínios que contêm imagens de abuso sexual de crianças (80% para fins comerciais e 20% para fins não-comerciais). Já em 2017 os relatórios de locais no Ciberespaço com material de abuso sexual de menores ascenderam a 5.439, verificando-se, contudo, que desde 2014 existe uma diminuição de imagens de crianças aparentando uma idade inferior a 10 anos (80% em 2014 e 55% em 2017), o que é um indicador positivo, pese embora tenham sido disponibilizadas imagens de maior violência sexual contra as crianças (8% para fins comerciais e 92% para fins não-comerciais). Por esta

instituição foram ainda detetadas, em 2017, 78.589 páginas web com material de abuso sexual de menores.

Constata-se, assim, que milhares de novas fotografias e vídeos são carregados para a Internet e todos os dias são realizadas centenas de milhares de pesquisas na *Web* para imagens de exploração sexual de crianças. É possível que existam pessoas que tenham em seu poder coleções de mais de um milhão de imagens de crianças vítimas de exploração sexual. Contudo, uma vez que a pornografia infantil é ilegal e objeto de perseguição penal na maioria dos países, é difícil calcular o número de menores que em todo o mundo são vítimas dessas redes, embora as estimativas indiquem entre 10.000 a 100.000 crianças de todas as idades.

O material de abuso sexual de menores ou é produzido *off-line* para posterior circulação na Internet ou é produzido em tempo real, para espetadores *on-line*. A produção e distribuição de material de abuso sexual de menores têm um valor estimado pela ONU entre US $3.000.000.000 e US $20.000.000.000 de dólares americanos (2009, p. 10). Acresce que as imagens disponíveis *on-line* de crianças exploradas sexualmente, além de crescerem em número, são cada vez mais violentas, pelo que as medidas de combate a este fenómeno, de caráter legal e operacional, se afiguram urgentes tendo em conta o número de vítimas em causa e o efeito que este tipo de práticas provoca nas crianças e na sociedade.

Em síntese, a cooperação entre organizações potenciou bons resultados mas a persistência e o crescimento do fenómeno justificam a intensificação de tal cooperação e o romper de novos caminhos pelo caráter nefasto de que se reveste a exploração sexual de uma só criança que seja. O fenómeno e o *locus* em questão exigem dos ISP um papel sem alternante.

Uma vez que este fenómeno criminal está associado ao Ciberespaço e à Internet, sendo a mobilidade destes serviços e alojamentos, permitida pela computação em *Cloud*, aos ISP deve ser atribuído o papel principal na monitorização e reporte dos conteúdos relacionados com a exploração sexual de crianças.

Nos Estados Unidos e na Austrália, por exemplo, estão previstas sanções para os prestadores de serviços de Internet e proprietários de domínio que não reportarem *sites* com conteúdos de abuso sexual de menores às autoridades de investigação, num prazo razoável. Na África do Sul um ISP deve tomar todas as medidas necessárias para prevenir a utilização dos seus serviços para hospedar ou distribuir material relacionado com a exploração sexual de crianças – o ISP deve notificar essa atividade às autoridades de investigação, bem como os dados da comunicação associada – nome e IP – para além ser obrigado a manter também um registo dessa informação para utilização como prova em processos criminais.

Os ISP localizados na África do Sul estão também obrigados por lei a tomar medidas para bloquear a divulgação deste tipo de imagens. Na Finlândia e na Suécia, a polícia pode bloquear *sites* de pornografia infantil, com o objetivo de impedir a circulação de imagens de exploração sexual de crianças.

III. Como Prevenir?

Como referência legal em textos internacionais quanto à segurança dos mais novos no Ciberespaço, há que referir a Lei de Proteção à Privacidade Online para Crianças de 1998 — The *Children's Online Privacy Protection Act* 1998 (COPPA) — que é uma lei federal dos Estados Unidos da América, promulgada em 21 de outubro de 1998 e que entrou em vigor em 21 de julho de 2000.

Esta legislação aplica-se à recolha *on-line* de informações pessoais por pessoas ou entidades sob jurisdição dos EUA relativamente a crianças menores de 13 anos de idade.

A lei especifica que um responsável por um *website* deve incluir uma política de privacidade que preveja quando e em que termos é necessário recolher o consentimento, verificável, por parte de um pai ou de um responsável pela criança, e quais as responsabilidades que impendem sobre um operador da Internet para proteger a privacidade e segurança *on-line* das crianças, incluindo restrições à comercialização de dados de crianças com idade inferior a 13 anos.

Embora crianças com idade inferior a 13 anos de idade possam fornecer informações pessoais, desde que tenha sido obtido o consentimento dos seus pais, muitos *sites* - especialmente as redes sociais (v.g. *Facebook*) – não permitem que crianças menores de idade utilizem os seus serviços devido ao custo e cautelas decorrentes para o pleno cumprimento desta lei.

A COPPA tem gerado alguma controvérsia nos Estados Unidos da América e tem sido criticada como ineficaz e potencialmente inconstitucional por especialistas legais e meios de comunicação de massa, desde que foi elaborada. As objeções referem, em síntese, que a legislação «encoraja fraudes de idade e permite que *sites* ignorem o ónus de obter consentimento dos pais». Ou seja, as restrições de idade e o processo de *«consentimento dos pais»* são fáceis de contornar, e os pais geralmente ajudam as crianças a mentir sobre a sua idade.

Por outro lado, as multas decorrentes da aplicação da COPPA (US $40.000,00 por violação) podem ser potencialmente catastróficas para as pequenas empresas, prejudicando o seu modelo de negócio. Enquanto as empresas maiores têm dinheiro suficiente para pagar a multa ou implementar um mecanismo de consentimento dos pais, as pequenas empresas geralmente não conseguem custear a implementação deste tipo de funcionalidades.

Mark Zuckerberg, co-fundador e CEO do *Facebook*, expressou a sua oposição à COPPA, referindo que se deve, sobretudo, apostar na educação dos mais novos, tendo declarado: *«Esta é uma luta que vamos assumir em algum momento. A minha filosofia é a de que, para a educação nesta área, é desejável que as crianças comecem o mais cedo que for possível»* (LEV-RAM, 2011).

Não obstante concordarmos que se deve investir sobretudo na educação dos mais novos quanto aos perigos que existem no Ciberespaço, com a capacitação de pais, de educadores e das escolas, é indiscutível que a legislação não deve ser neutra quanto à recolha de dados pessoais das crianças e adolescentes, no sentido de alertar os mais incautos, incluindo pais e educadores quanto aos riscos existentes e em ordem a proteger os seus dados pessoais e a reserva da sua vida privada, direito a ser respeitado inclusive pelos pais (CALVÃO, 2016).

A este propósito decidiu, e bem, o acórdão do Tribunal da Relação de Évora (TRE, 2015) quando determinou que *«a imposição aos pais do dever de abster-se de divulgar fotografias ou informações que permitam identificar a filha nas redes sociais mostra-se adequada e proporcional à salvaguarda do direito à reserva da intimidade da vida privada e da proteção dos dados pessoais e, sobretudo, da segurança da menor no Ciberespaço»*, decisão que foi proferida relativamente a uma criança de 2 anos de idade, no âmbito de um processo de regulação do exercício das responsabilidades parentais, inexistindo acordo entre os pais em relação a este tema. A questão suscitada no recurso era apenas jurídica e consistia em saber se existe fundamento legal e factual para o tribunal impor a obrigação dos progenitores se absterem «*de divulgar fotografias ou informações que permitam identificar a filha nas redes sociais».* Referiu o Tribunal da Relação de Évora o seguinte *«(…)e conhecendo, diremos que a apelação é manifestamente improcedente, porquanto o segmento da decisão que vem impugnado não carece de fundamentação de facto específica para justificar a adoção daquela medida. Ela é uma obrigação dos pais, tão natural quanto a de garantir o sustento, a saúde e a educação dos filhos e o respeito pelos demais direitos designadamente o direito à imagem e à reserva da vida privada (art.º 79º e 80º do CC). Na verdade, os filhos não são coisas ou objetos pertencentes aos pais e de que estes podem dispor a seu belo prazer. São pessoas e, consequentemente, titulares de direitos. Se, por um lado, os pais devem proteger os filhos, por outro, têm o dever de garantir e respeitar os seus direitos. É isso que constituiu o núcleo dos poderes/*deveres *inerentes às responsabilidades parentais e estas devem ser sempre norteadas, no «superior interesse da criança», que se apresenta, assim, como um objetivo a prosseguir por todos quantos possam contribuir para o seu desenvolvimento harmonioso: os pais, no seu papel primordial de condução e educação da criança; as instituições, ao assegurar a sua tutela e o Estado, ao adotar as medidas tendentes a garantirem o exercício dos seus direitos e a sua segurança».*

De referir, ainda, em termos de enquadramento legal que o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, prescreve que o tratamento de dados pessoais no âmbito da sociedade da informação só é lícito se as crianças forem maiores de 16 anos. Caso a criança seja menor de 16 anos, esse tratamento só é lícito se, e na medida em que, o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança, de acordo com a legislação nacional, mas as crianças nunca podem ter idade inferior a 13 anos. Ou seja, há uma proibição geral de tratamento de dados de crianças no âmbito da sociedade da informação, caso estas tenham idade inferior a 13 anos. Sobre esta temática pronunciou-se a CNPD — Comissão Nacional de Proteção de Dados (Parecer, CNPD, 2018) sobre a Proposta de Lei n.º 120/XIII/3.ª (Gov)

que «*Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito aos tratamentos de dados pessoais e à livre circulação desses dados*» propugnando que, estando em causa determinar a partir de que idade se reconhece ter uma criança capacidade para consentir na restrição a um direito fundamental, seria porventura expectável que na proposta se tomasse por referência o critério fixado no Código Penal, no artigo 38.º, n.º 3, quanto ao consentimento como causa de exclusão da ilicitude penal: 16 anos.

Podem ser configuradas regras informais de atuação no Ciberespaço, que podem ser consensualizadas entre pais e filhos, e eventualmente em sede de processo de promoção e proteção (cfr. artigos 55.º e 56.º da Lei n.º 147/99, de 1 de Setembro), caso se justifique, e quanto à utilização responsável das TIC, indicando-se alguns exemplos de cláusulas (COSTA, Para os Pais):

1. Posso usar a internet das…… às ….h, (tempo) por dia/semana para entretenimento (jogos, consulta de sítios, redes sociais).

2. A senha das redes sociais é do conhecimento dos meus pais, mas nunca dos meus amigos.

3. Só visitarei sítios autorizados pelos meus pais.

4. Se quiser comprar algo *online*, peço aos meus pais para efetuarem a compra.

5. Comunico aos meus pais se for abordado(a) de forma inapropriada por alguém (palavrões, convites, conversas intimas, fotografias ou imagens de conteúdo sexual) ou se me sentir incomodado(a) com alguma coisa.

6. Tenho noção que os amigos das redes sociais são só amigos virtuais e podem não ser quem dizem. Só marcarei encontro com alguém, excecionalmente, se os meus pais souberem e autorizarem.

7. O meu endereço, número de telefone/telemóvel, escola e locais que frequento ou a minha senha de acesso não são para partilhar na net.

8. Só posso colocar fotografias autorizadas pelos meus pais.

9. Devo respeitar os outros e não fazer comentários depreciativos ou maldosos sobre ninguém.

10. Estas regras também se aplicam ao meu … (telemóvel, Tablet, etc.).

As entidades com competência em matéria de infância e juventude — entidades, públicas ou privadas, que estão, por força das suas funções, em contacto com a criança ou jovem,

designadamente a escola, o sistema de saúde, a Segurança Social, ONGs, etc. – as Comissões de Proteção de Crianças e Jovens, o Ministério Público e os Tribunais, que desenvolvem o seu trabalho na área da família e das crianças devem ter uma atitude pedagógica e construtiva perante esta realidade, orientando também as suas decisões em ordem a proteger os dados pessoais, a reserva da vida privada e a segurança das crianças e jovens no Ciberespaço, porque tal lhe é, além do mais, legalmente imposto.

Efetivamente, estes cuidados visam acautelar os efeitos decorrentes da distribuição do material de abuso na Internet ou de utilização indevida dos dados pessoais dos mais novos, que são, nos casos de abuso, suscetíveis de agravar as consequências do abuso infantil, afetando a recuperação integral das vítimas – as imagens das crianças exploradas sexualmente e divulgadas na Internet, podem de facto nunca desaparecer e essa circunstância tem um efeito nefasto sobre as vítimas, necessitando de mais tempo e esforço para recuperar da violência a que foram sujeitas. A recuperação é agravada pelo medo de que algo de tão pessoal que sucedeu no passado, possa reaparecer em qualquer lugar, a qualquer momento e ser visto por qualquer pessoa. Esta circunstância constitui uma violação sem fim do direito à privacidade, que provoca uma humilhação adicional nas vítimas, que crescem conhecendo que aquelas fotografias ou vídeos estarão na Internet para o resto das suas vidas.

Perante a constatação da dificuldade em combater este fenómeno, e independentemente das obrigações legais, um número crescente de ISPs operadores de telecomunicações móveis e instituições financeiras de países estrangeiros têm adotado códigos de conduta numa tentativa de autorregulação associada à repressão da distribuição de material de abuso sexual de menores, reportando esses conteúdos à IC. Ou seja, uma vez que este fenómeno criminal está associado ao Ciberespaço e à Internet, aos ISP deve ser atribuído o papel principal na monitorização e reporte dos conteúdos relacionados com a exploração sexual de crianças.

Em Portugal não está ainda estabelecida (!) a obrigatoriedade específica de os ISP monitorizarem conteúdos para detetar aqueles que são afins da exploração sexual de crianças e, por isso, não está legalmente prevista nenhuma sanção caso os ISP não reportem a existência de material de exploração sexual de menores na Internet. Tendo em conta as características deste fenómeno, as obrigações do Estado Português perante convenções internacionais em vigor no ordenamento jurídico português, a dimensão do fenómeno e as consequências deste tipo de práticas para as vítimas, torna-se premente estabelecer a obrigatoriedade do reporte de tais tipos de conteúdos às Autoridades de IC, designadamente ao Ministério Público e assegurar, em articulação com as instituições financeiras, o bloqueio de pagamentos relacionados com a comercialização deste tipo de material.

Nesse sentido, propugna-se a construção de uma Estratégia Nacional Integrada de Proteção das Crianças Contra a Violência, tendo como referencial as *Orientações do Conselho da Europa sobre estratégias nacionais integradas para a proteção das crianças contra a violência* (*Council of Europe*). A concretização dessa estratégia poderia basear-se na construção de planos nacionais de proteção das crianças contra a violência, de caráter

multidisciplinar e integrado, com a participação de entidades privadas e públicas, nomeadamente das áreas da Justiça, da Segurança da Social, da Saúde, da Administração Interna, da Educação e, eventualmente, cooperação com organizações internacionais, nomeadamente empresas das TIC.

Em suma, a coordenação e articulação entre as autoridades dos diversos países, a partilha de recursos humanos e técnicos e de informação sobre o fenómeno, e um compromisso coletivo a nível nacional e internacional, envolvendo parceiros públicos e privados, são fatores indispensáveis para possibilitar políticas de prevenção e proteção mais eficazes e, assim, garantir maior segurança para os mais novos no Ciberespaço, não olvidando a necessidade imperiosa de capacitar pais e educadores quanto aos riscos e perigos existentes.

IV. Potencialidades e oportunidades no Ciberespaço

Com previsão notável, William Gibson, em 1984, no romance "*Neuromancer*" (Gibson, 1984, p. 12) previu que a crescente dependência da sociedade dos computadores e tecnologias de informação criaria um universo virtual eletrónico, a que denominou Ciberespaço. Poucos anos mais tarde, o Ciberespaço tornou-se muito mais do que uma premissa, uma ficção ou romance. A Internet, rapidamente e com surpresa, tornou-se comum na vida diária e cada vez mais vital para a aquisição de conhecimento e comunicação entre pessoas de todo o mundo.

A partir destas considerações, o termo "Ciberespaço" pode ser definido como *locus* virtual criado pela conjunção das diferentes tecnologias de telecomunicação e telemática, em especial, mas não exclusivamente, as mediadas por computador. É importante sublinhar que essa definição não circunscreve o Ciberespaço às redes de computadores, mas abarca as diferentes formas de comunicação da Informação, desde teleconferências analógicas, passando por redes de computadores, "*pagers*", comunicação entre radioamadores e por serviços do tipo "tele-amigos" ou redes sociais.

A Internet, apesar de ser a mais presente, não é a única instância de CMC, e por extensão, de suporte ao Ciberespaço. Atualmente percebe-se uma tendência de unificação da esfera global de telecomunicações a partir de plataformas digitais, seja a partir da rede Internet "pública" ou de outro tipo de redes e dispositivos. A Internet é a rede das redes, na medida em que constitui verdadeiramente uma rede global e integrante. É um sistema global de redes de computadores interconectadas, que usam um conjunto standard de protocolos de comunicação, o *Transmission Internet Protocol* (TCP/IP). Esta rede é constituída por milhões de redes de computadores privados, públicos, de empresas, de governos, faculdades, entre outras instituições, que estão ligadas entre si através de tecnologias de rede diversas. A Internet disponibiliza uma série de serviços e protocolos como são os casos da *World Wide Web* (WWW) http, https, ftp e ftps, ou da infraestrutura de suporte ao correio eletrónico com recurso a SMTP, POP e IMAP, a título exemplificativo.

Uma das revoluções que se encontra atualmente em curso é a denominada Internet das Coisas, também conhecida pelo acrónimo IoT, e parte do princípio de que todos os aparelhos e objetos que se encontram habilitados a estarem permanentemente ligados à Internet, são capazes de se identificar na rede e de comunicar entre si. Podem ter o seu estado alterado através daquele meio, com ou sem o envolvimento ativo do ser humano e têm capacidade para recolher uma vasta quantidade de informação sobre os que os rodeiam. A Internet *Society* define o IoT em sentido amplo como «a extensão da conectividade de rede e capacidade de computação para objetos, dispositivos, sensores e outros artefactos que normalmente não são considerados computadores». Veículos, luzes de trânsito, eletrodomésticos, câmaras de vigilância, detetores de condições ambientais, sensores de presença, e dispositivos médicos são apenas alguns exemplos do que já hoje existe no universo IoT (LEVEREGE, 2018).

O objetivo (benigno) de todos estes dispositivos e sobretudo da grande quantidade de dados resultantes da respetiva interação através da Internet, é que o processamento resultante seja efetuado para que, por exemplo, se evitem engarrafamentos de trânsito, se antecipe atempadamente uma doença fatal num doente ou um incidente num edifício, se utilize de forma mais eficiente a energia, para dar apenas alguns exemplos.

Relativamente à Indústria 4.0, também conhecida por *Industry IOT* (IIoT), o conceito vai muito para além da mera implantação de sistemas eletrónicos e de TICs em geral nos processos de produção nas fábricas, que caracterizou a Indústria 3.0.

Esta nova vaga tecnológica, que se baseia no conceito acima explanado sobre a IoT, viabiliza uma grande interação entre os diversos dispositivos instalados ao longo da cadeia de produção no «chão de fábrica», incluindo a cadeia logística, proporcionando que os processos de fabrico resultem de uma comunhão entre o mundo físico e o virtual. Quer os equipamentos nas linhas de produção, quer os produtos que estão a ser fabricados, quer os centros logísticos são capazes de interagir autonomamente, mais uma vez com o objetivo (benigno) de melhorar o processo produtivo e assim fabricar produtos de maior qualidade, mais alinhados com os requisitos do cliente e com uma melhorada eficiência em toda a cadeia de valor. Por outras palavras, a tecnologia digital em que se baseia a Indústria 4.0, quer na componente de produção quer na componente logística, contempla a simbiose da informação digital proveniente de várias fontes e locais, tendo em vista o comando e controlo do ato físico de produzir e distribuir um bem ou conjunto de bens. Esta união dos sistemas TIC com as OT (*Operational Technologies*) é caracterizada por uma forte interação digital-físico-digital, envolvendo um conjunto de tecnologias que vão muito para além do IoT, como é o caso da análise massiva de dados (*Big Data & Analytics*), impressão 3D, robótica e inteligência artificial, entre outros, e que completam o ciclo que digitaliza todo o processo produtivo e logístico.

Assim, a IoT é uma realidade inexorável e irá progressivamente invadir o espaço onde trabalhamos, onde nos divertimos e onde vivemos todos os dias (LEVEREGE, 2018).

Em conclusão, o Ciberespaço oferece ao mundo e às sociedades potencialidades capazes de fomentar o desenvolvimento sociocultural, económico, científico e tecnológico. A partir das diversas redes, de qualquer ponto ou terminal, é possível contactar com o resto do mundo. Recolher e enviar informação, aprofundar e promover estudo, desenvolver atividade profissional e gerir empresas, entre outros aspetos, tudo é possível, embora a interação, sobretudo dos mais novos, e eventualmente dos adultos, deva ser feita com cautelas e segurança, face aos perigos existentes.

V. Conclusões

A exploração sexual de crianças no Ciberespaço constitui hodiernamente um problema mundial. A sua expressão assume formas diversas. O comércio de material com imagens de abuso sexual de menores continua a crescer a uma velocidade alarmante. A utilização de computadores e de tecnologia de diversa natureza (correio eletrónico, *sites* comerciais, salas de conversação *online*, aplicações *peer-to-peer*, *webcams)* para cometer crimes relacionados com a exploração sexual de crianças e a utilização indevida de dados pessoais dos mais novos está em crescendo, não tem fronteiras e ocorre em tempo tendencialmente instantâneo. Como fator potenciador do fenómeno assinala-se o recato potenciado pelo uso da Internet e o informalismo da comunicação. Os mais jovens, movidos pela curiosidade, são especialmente vulneráveis e incautos (por inexperiência de vida), suscetíveis de serem facilmente atraídos para uma situação de exploração sexual ou de exposição da sua vida privada, sem consciência do significado e consequências dos seus comportamentos. Efetivamente, perante menores pouco informados dos perigos existentes no Ciberespaço contrapõem-se redes internacionais de produtores, comerciantes e colecionadores de imagens de crianças com conteúdo sexual, muitas vezes ligados ao crime organizado (traficantes de produtos estupefacientes, traficantes de armas, traficantes de pessoas, etc.) e ao branqueamento de capitais – este tipo de organizações criminosas, a partir de um simples terminal de acesso à Internet, têm facilidade de acesso a um universo mundial de consumidores.

No Ciberespaço não existem fronteiras e pretender conter a comunicação a um espaço nacional é objetivo "fracassado", pelo que as imagens e dados pessoais circulam livremente dos fornecedores de material para os consumidores, sem ser necessário um encontro pessoal ou uma entrega física, por contraposição, em certa medida, ao tráfico de droga ou ao contrabando de tabaco.

Os produtores, comerciantes e os colecionadores de material de abuso sexual de menores atuam predominantemente a coberto do anonimato e podem ser encontrados em qualquer país, pelo que todos os países, incluindo pais, professores e escolas devem desenvolver esforços para prevenir e reprimir com eficácia este tipo de criminalidade, se mais não fora porque as crianças são o nosso futuro que, para ser sustentável, carece de pessoas saudáveis.

A investigação de quem no ciberespaço desenvolve atividades conexas com a exploração sexual de crianças está confrontada com a dificuldade de rastreio das máquinas que veicularam a atuação dos criminosos.

A colaboração dos ISP e das instituições cuja atividade consista na disponibilização de serviços e ou monitorização de conteúdos no Ciberespaço é de extrema relevância na prevenção, deteção e repressão deste fenómeno. À semelhança dos EUA e da Austrália, deverão ser previstas sanções para os ISP e proprietários de domínio que não reportem, às autoridades de IC, *sites* com conteúdos de abuso sexual de menores.

A investigação deste tipo de criminalidade e a dedução da acusação em processo penal deve ser facilitada pela legislação e pela adaptação operacional das autoridades de IC. Nesse sentido, é necessário promover a implementação de medidas adotadas internacionalmente e preconizadas em textos internacionais subscritos por Portugal, que garantam:

- A supressão imediata das páginas eletrónicas que contenham ou difundam material de abuso sexual de menores sediadas em território nacional, preservando-se os respetivos registos de criação, acesso e manutenção para cedência às autoridades IC, em articulação com os ISP e outras entidades de monitorização de conteúdos no Ciberespaço;

- O bloqueio imediato do acesso a páginas eletrónicas que contenham ou difundam material de abuso sexual de menores localizadas fora do território nacional, em articulação com os ISP e outras entidades de monitorização de conteúdos no Ciberespaço;

- A comunicação das referências de *websites* com material de abuso sexual de menores detetadas pela IC aos ISP, às entidades de monitorização de conteúdos no Ciberespaço e entidades financeiras, de forma a operacionalizar o bloqueio e acesso aos respetivos conteúdos, e outrossim permitir que as entidades bancárias possam impedir pagamentos através de cartões de débito e crédito pela utilização e visualização desse material. Esta divulgação exigiria forte cooperação judiciária internacional em matéria penal, sob pena de os esforços de um país serem manifestamente inúteis, face à ausência de fronteiras no Ciberespaço e à diversidade de jurisdições envolvidas;

- A comunicação por parte dos ISP e de outras entidades que desenvolvam a sua atividade no Ciberespaço às autoridades de IC de *sites* com material de abuso sexual de menores;

- A comunicação por parte de entidade bancárias dos pagamentos efetuados com cartões de débito e de crédito associados a *sites* com material de abuso de menores às autoridades de IC;

- A vigilância preventiva de conteúdos no Ciberespaço tendente a identificar material de abuso sexual de menores;

- O desenvolvimento e incremento de ações encobertas direcionadas para a prevenção e investigação criminal deste fenómeno;

- A construção de uma base de dados, tutelada pelas autoridades de IC, com material relacionado com o abuso sexual de menores, apreendido nas investigações, transmitidos ou disponibilizados através de tecnologias de informação ou comunicação, como fotografias, vídeos e identificação de *websites*, que permitisse, através da análise de dados, identificar vítimas, agressores, recursos do Ciberespaço (locais) e a troca de informação com entidades de IC estrangeiras, designadamente a Eurojust, a Europol e a Interpol;

- A construção de capacidades operacionais de tratamento e análise centralizado de informação, recolhida no âmbito da prova digital tratada em sede de processos-crime relacionados com a exploração sexual de crianças no Ciberespaço e sua posterior disseminação pelas autoridades de IC, nacionais e estrangeiras, em articulação com a atividade de prevenção criminal e de educação dos mais novos, incluindo pais e professores.

As medidas elencadas permitiriam debelar as dificuldades com que a IC se debate na investigação do fenómeno da exploração sexual de crianças no Ciberespaço, em prol da eficácia na prossecução de um objetivo comum – a proteção das crianças contra a violação da sua vida privada e exploração sexual. Das medidas elencadas merece destaque, pela globalidade do fenómeno, a intensificação da cooperação internacional neste domínio.

Perante a constatação da dificuldade em combater este fenómeno, e independentemente das obrigações legais, um número crescente de ISPs operadores de telecomunicações móveis e instituições financeiras de países estrangeiros têm adotado códigos de conduta numa tentativa de autorregulação associada à repressão da distribuição de material de abuso sexual de menores, reportando esses conteúdos à IC. Ou seja, uma vez que este fenómeno criminal está associado ao Ciberespaço e à Internet, aos ISP deve ser atribuído o papel principal na monitorização e reporte dos conteúdos relacionados com a exploração sexual de crianças.

Todos estes exemplos estão alinhados, na prática, com a norma ISO 26000 sobre a responsabilidade social das organizações, em prol de um desenvolvimento sustentável da sociedade. A ISO 26000 é um padrão de orientação de atuação, aplicável a todos os tipos organizações, o que significa que não é suscetível de certificação. A responsabilidade social é definida como a assunção da responsabilidade por parte das organizações pelos impactos das suas decisões na sociedade e no meio ambiente, preconizando que as organizações, no âmbito da sua atuação interna e externa, devem orientar a sua atividade tendo

sempre em consideração o respeito pelos direitos humanos. No ponto 6.3. da ISO 26000 considera-se que as organizações têm a responsabilidade de respeitar todos os direitos humanos, independentemente de o Estado ser capaz ou não desejar cumprir com seu dever de protegê-los. Essa responsabilidade envolve tomar medidas positivas para evitar a aceitação passiva ou a participação ativa na violação de direitos. Cumprir com a responsabilidade de respeito dos direitos humanos requer diligência e pro-atividade por parte das organizações, que deverão promover a adoção de medidas adicionais, no sentido de assegurar que respeitam os direitos humanos em todas as suas operações.

No âmbito da referida norma da qualidade preconiza-se, em especial, que as organizações e as empresas tenham em conta a proteção conferida às crianças pelos instrumentos da ONU, adotando códigos de conduta e boas práticas de negócio tendentes à proteção das crianças contra violação dos seus dados pessoais. Esta abordagem deve ser considerada nas organizações nacionais, sobretudo aquelas cuja atividade está relacionada com o Ciberespaço (eg.: ISP, empresas de comunicações, instituições financeiras, fornecedores de serviços de *wifi*, organizações privadas e públicas), independentemente das suas obrigações legais atuais e futuras (*Ecpat Sweden Briefing Paper*, 2011).

Nesse sentido, propugna-se a construção de uma Estratégia Nacional Integrada de Proteção das Crianças e Jovens Contra a Violência, tendo como referencial as *Orientações do Conselho da Europa sobre estratégias nacionais integradas para a proteção das crianças contra a violência* (*Council of Europe*). A concretização dessa estratégia poderia basear-se na construção de planos nacionais de proteção das crianças contra a violência, de caráter multidisciplinar e integrado, com a participação de entidades privadas e públicas, nomeadamente das áreas da Justiça, da Segurança Social, da Saúde, da Administração Interna, da Educação e, eventualmente, cooperação com organizações internacionais, nomeadamente empresas das TIC.

Pese embora, concordemos que se deve investir sobretudo na educação dos mais novos quanto aos perigos que existem no Ciberespaço, com a capacitação de pais, de educadores e das escolas, é inquestionável que a legislação não deva ser neutra quanto à recolha de dados pessoais das crianças e adolescentes, no sentido de alertar os mais incautos, incluindo pais e educadores quanto aos riscos existentes e em ordem a proteger os dados pessoais e a reserva da sua vida privada, direito a ser respeitado inclusive pelos pais (CALVÃO, 2016).

A este propósito decidiu de forma inovadora o acórdão do Tribunal da Relação de Évora (TRE., 2015) quando determinou que *«a imposição aos pais do dever de abster-se de divulgar fotografias ou informações que permitam identificar a filha nas redes sociais mostra-se adequada e proporcional à salvaguarda do direito à reserva da intimidade da vida privada e da proteção dos dados pessoais e, sobretudo, da segurança da menor no Ciberespaço»*, decisão que foi proferida relativamente a uma criança de 2 anos de idade, no âmbito de um processo de regulação do exercício das responsabilidades parentais, inexistindo acordo entre os pais em relação a este tema.

De referir, ainda, em termos de enquadramento legal que o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, prescreve que o tratamento de dados pessoais no âmbito da sociedade da informação só é lícito se as crianças forem maiores de 16 anos. Caso a criança seja menor de 16 anos, esse tratamento só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança, de acordo com a legislação nacional, mas as crianças nunca podem ter idade inferior a 13 anos. Ou seja, há uma proibição geral de tratamento de dados de crianças no âmbito da sociedade da informação, caso estas tenham idade inferior a 13 anos, preconizando a CNPD que essa proibição se deveria ter em consideração a idade de 16 anos (Parecer, CNPD, 2018), de acordo com opção facultada pelo Regulamento.
Não obstante os riscos acima assinalados, é inquestionável que o Ciberespaço oferece ao mundo e às sociedades potencialidades capazes de fomentar o desenvolvimento sociocultural, económico, científico e tecnológico. A partir das diversas redes, de qualquer ponto ou terminal, é possível contactar com o resto do mundo. Recolher e enviar informação, aprofundar e promover estudo, desenvolver atividade profissional e gerir empresas, entre outros aspetos, tudo é possível, embora a interação, sobretudo dos mais novos, e também dos adultos, deva ser feita com conhecimento, consciência dos riscos, cautelas e segurança, face aos perigos existentes.

Siglas e Abreviaturas

Ac. – Acórdão
CMC – Comunicações Mediadas por Computador
DNS – Domain Name System
ECPAT – End Child Prostitution, Child Pornography and the Traficking of Children for Sexual Purposes
EUA – Estados Unidos da América
FTP – File Transfer Protocol ou protocolo de transferência de ficheiros
HTML – HyperText Markup Language
IC – Investigação Criminal
IoT – Internet das Coisas
IP – Internet Protocol
ISP – Internet Service Provider
IWF – Internet Watch Foundation
P2P – Peer-to-Peer
SI – Sistemas de Informação
TIC – Tecnologias de Informação e Comunicação
TRE – Tribunal da Relação de Évora
URL – Uniform Resource Locator
WWW – World Wide Web.

Bibliografia

Ac. do TRE, de 2016-06-25 – **Regulação das responsabilidades parentais.Cibercrime**. [Em Linha]. Proc. 789/13.7TMSTB-B.E1. Des. Bernardo Domingos et al.. [Consult. 2018-05-10]. Disponível em WWW: <URL: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/7c52769f1dfab8be80257e830052d374?OpenDocument&Highlight=0,ciberespa%C3%A7o>.

CALVÃO, Filipa Urbano – **Anotação ao Acórdão da Relação de Évora de 25 de Junho de 2015 – Regulação das Responsabilidades Parentais e Cibercime.** Forum de Proteção de dados, n.º 2, 2016. ISSN 2183-7066 [Em Linha]. [Consult. 2018-05-11]. Disponível em WWW: <URL:https://www.cnpd.pt/bin/revistaforum/forum2016_2/files/assets/basic-html/page-126.html>, págs. 127 a 135.

CARR, John, e Hilton, Zoë - **Coalition on Internet Safety: Digital Manifesto – Action for Children**. [Em Linha]. London, 2009, p. 29. [Consult. 2012-04-07]. Disponível em WWW: <URL: www.chis.org.uk/uploads/02b.pdf>.

CNPD — Comissão Nacional da Proteção de Dados – **Parecer n.º 20/2018 Assembleia da República Comissão de As. Constitucionais, Direitos, Liberdades e Garantias** – [Em Linha]. [Consult. 2018-05-11]. Disponível em WWW: <URL: https://www.cnpd.pt/bin/decisoes/Par/40_20_2018.pdf>, págs. 17 e 17 v.

COSTA, Ana Rodrigues da – **Para os Pais**: **10 regras para a utilização da Internet.** [Em Linha]. [Consult. 2018-05-11]. Disponível em WWW: <URL:https://www.portoeditora.pt/paisealunos/para-os- pais/noticia/ver/?id=78284&langid=>.

ECPAT – End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes, Sweden – **The Commercial Sexual Exploitation of Children**, 1.ª ed., Stockholm: ECPAT Sverige an Jurge Forlag AB, 2011 - ISBN 978-91-7223-447-5, pág. 154.

EUROPE, Council – **Council of Europe Guidelines on Integrated national strategies for the protection of children from violence.** [Em Linha]. [Consult. 2018-05-11]. Disponível em WWW: <URL: https://rm.coe.int/168046d3a0>.

GIBSON, William – **Neuromancer**, The Berkley Publishing Group, a division of Penguin Putnam Inc. – New York, 1984.

IWF – Internet Watch Foundation, Annual and Charity Report, 2006 e 2010, Cambridge, UK, 2007 and 2011, (2007 e 2010) [Em Linha]. [Consult. 2012-04-05]. Disponível em WWW: <URL:www.enough.org/objects/20070412_iwf_annual_report_2006_web.pdf> e WWW: <URL:http://www.iwf.org.uk/assets/media/annualreports/Internet%20Watch%20Foundation%20Annual%20Report%202010%20web.pdf.

IWF – Internet Watch Foundation, Annual Report 2017, Cambridge, UK, (2017) [Em Linha]. [Consult. 2018-04-20]. Disponível em WWW:
<URL: https://annualreport.iwf.org.uk/#statistics_and_trends_2017>.

Lalor et al. [Em Linha]. [Consult. 2018-04-20]. Disponível em WWW:
<URL:https://www.coe.int/t/dg3/children/1in5/Source/PublicationSexualViolence/LalorMcElvaney.p>.
LEITE, Inês F.- Pedofilia - **Repercussões das Novas Formas de Criminalidade na Teoria Geral da Infracção**. 1.ª ed., Coimbra: Almedina, 2004, págs. 15 e 16.

LEVEREGE – **An Introduction to the Internet of things**, First Edition, 2018. [Em Linha]. [Consult. 2018-05-10]. Disponível em WWW:
<URL: https://indd.adobe.com/view/d38aec14-b884-492d-ba9f-de7ffe59ac6c>.

LEV-RAM, M. – **Zuckerberg: Kids under 13 should be allowed on Facebook** – Fortune. Time, Inc. Retrieved 22 June 2016. [Em Linha]. [Consult. 2018-05-11]. Disponível em WWW:
<URL:http://www.fortune.com/2011/05/20/zuckerberg-kids-under-13-should-be-allowed-onfacebook/>.

MAGRIÇO, Manuel Eduardo Aires Magriço - **A Exploração Sexual de Crianças no Ciberespaço**, 2014, Lisboa, Aletheia Editores- ISBN – 9789896226640.

ONU – Human Rights Council – **Report of the Special Rapporteur on the Sale of Children, Child Prostitution and Child Pornography**, Najat M'jid Maalla, (13-07-2009), A/HRC/12/23. [Em Linha]. [Consult. 2012-06- 21]. Disponível em WWW:
<URL:http://www.unhcr.org/refworld/docid/4ab0d35a2.html>.

TINK, Palmer e STACEY, Lisa - **Just One Click: Sexual abuse of children and young people through the Internet and mobile phone technology**, Barnardo´s, Ilford, UK – United Kingdom, 2004.

Vídeo da apresentação

➔ https://educast.fccn.pt/vod/clips/262y7b7hay/flash.html?locale=pt

CENTRO
DE ESTUDOS
JUDICIÁRIOS

2.

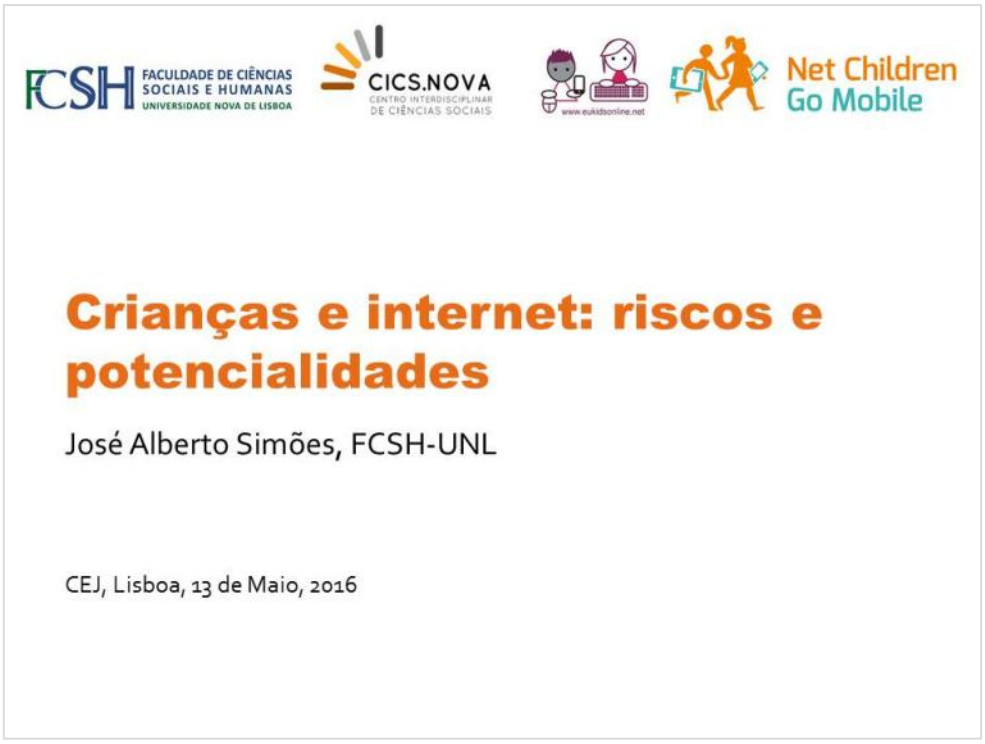
A Internet e as crianças – riscos e potencialidades

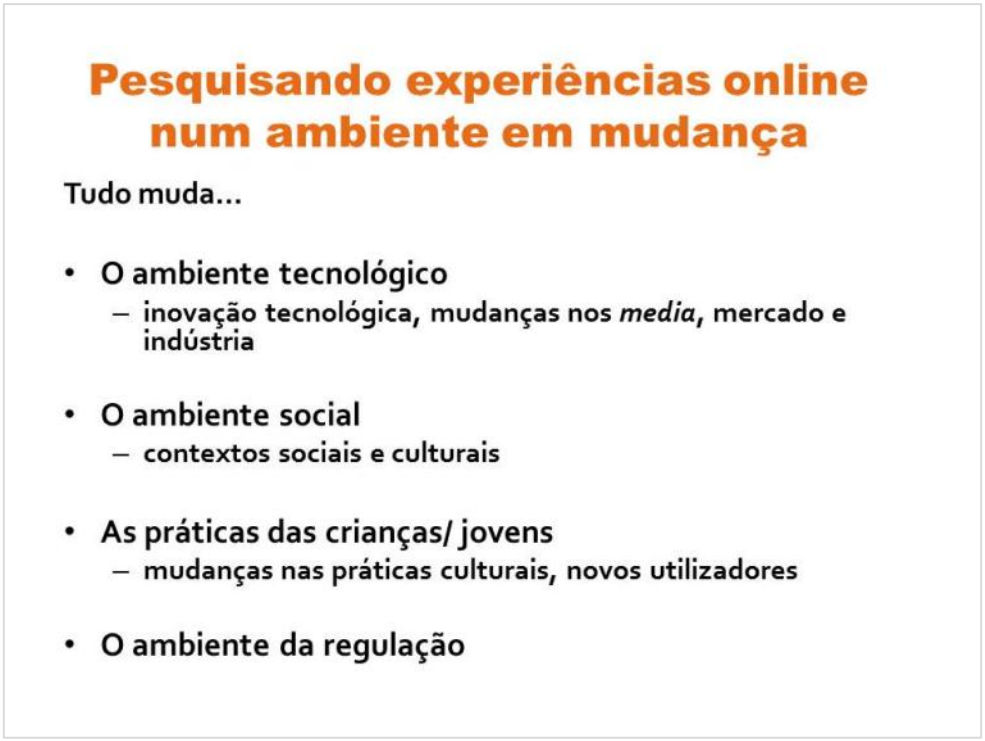
José Alberto Simões

CENTRO
DE ESTUDOS
JUDICIÁRIOS

CRIANÇAS E INTERNET: RISCOS E POTENCIALIDADES

José Alberto Simões*



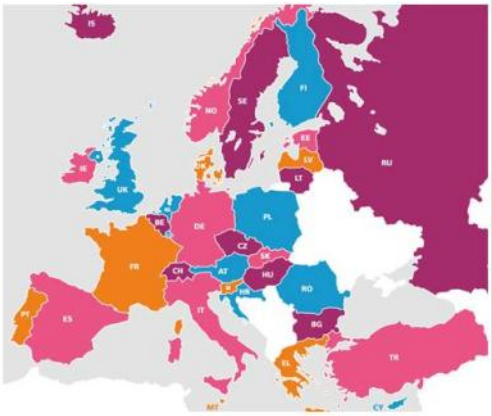


* Docente universitário da Universidade Nova de Lisboa.

Uma década de investigação
(financiada por 'EC Better Internet for Kids')

- Portugal participa desde **2006**
- Inquérito **EU Kids Online** (2010)
  25 países: 25 000 crianças/ jovens (9-16 anos) + um dos seus pais, entrevistados em casa
- Inquérito **Net Children Go Mobile** (2013-14)
  7 países: 3500 crianças/jovens (9-16 anos), entrevistados em casa
- Rede atualmente (2014-18) conta com **33 países**

Novo inquérito previsto para 2017

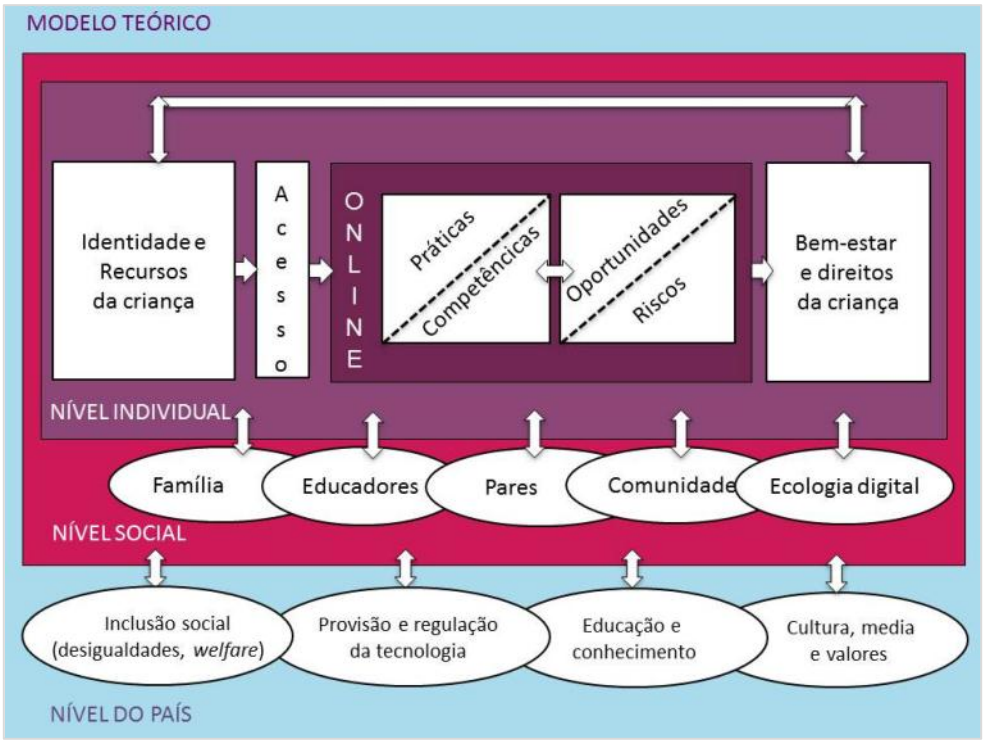


Definindo riscos

- Não existe uma definição única e consensual de riscos, dado que estes variam de acordo com:
  - o **contexto cultural,**
  - as **experiências** individuais,
  - e as **percepções** de cada um
- De modo a evitar as ansiedades e o 'pânico moral' à volta dos riscos é preciso distinguir:
  - as ***construções discursivas*** (dos *media*, do senso comum, etc.) das ***experiências efectivas*** de risco

Riscos e dano

- Riscos representam experiências **potencialmente negativas ou prejudiciais**
- Porém, **nem todas** as experiências potencialmente negativas se traduzem em dano
- Por outro lado, as experiências **arriscadas** (e as suas consequências possíveis) variam em **gravidade e intensidade**
- É preciso **correr riscos para obter oportunidades**
- Questão central: **como lidar com os riscos?**



Riscos e oportunidades

		Conteúdo: Criança como receptor	*Contacto: Criança como participante*	*Conduta: Criança como actor*
RISCOS	***Comerciais***	Publicidade, spam, patrocínios	Seguir/recolher informação pessoal	Apostas, dowloads ilegais, hacking
	Agressividade	Conteúdos violentos/macabros/ odiosos	Ser vítima de bullying, assédio ou perseguição	Exercer bullying ou assédio sobre outro
	Sexuais	Conteúdos pornográficos/ sexuais prejudiciais	Conhecer estranhos, namoros online	Criar/fazer upload de material pornográfico
	Valores negativos	Informação/conselhos racistas ou prejudiciais (e.g. drogas)	Auto-mutilação, persuasão indesejada	Fornecer conselhos e.g. sobre suicídio/pro-anorexia
OPORTUNIDADES	***Educação, aprendizagem e literacia digital***	Recursos educacionais	Contacto com outros que partilham os mesmos interesses	Aprendizagem por iniciativa própria ou colaborativa
	Participação e envolvimento cívico	Informação global	Troca entre grupos de interesses	Formas concretas de envolvimento cívico
	Criatividade e auto-expressão	Diversidade de recursos	Ser convidado/inspirado a criar ou participar	Criação de conteúdo gerado pelo usuário
	Identidade e relações sociais	Aconselhamento (pessoal/saúde/sexual etc)	Redes sociais, partilha de experiências com outros	Expressão de identidade

Projecto *Net Children Go Mobile* (2012-14)

- **Objectivo**: estudar as **alterações** introduzidas nas práticas online de crianças e jovens (9-16 anos), particularmente as que envolvem riscos, com o acesso crescente à internet através de **meios móveis e convergentes**
- Pesquisa realizada entre **2012-14** – países envolvidos:

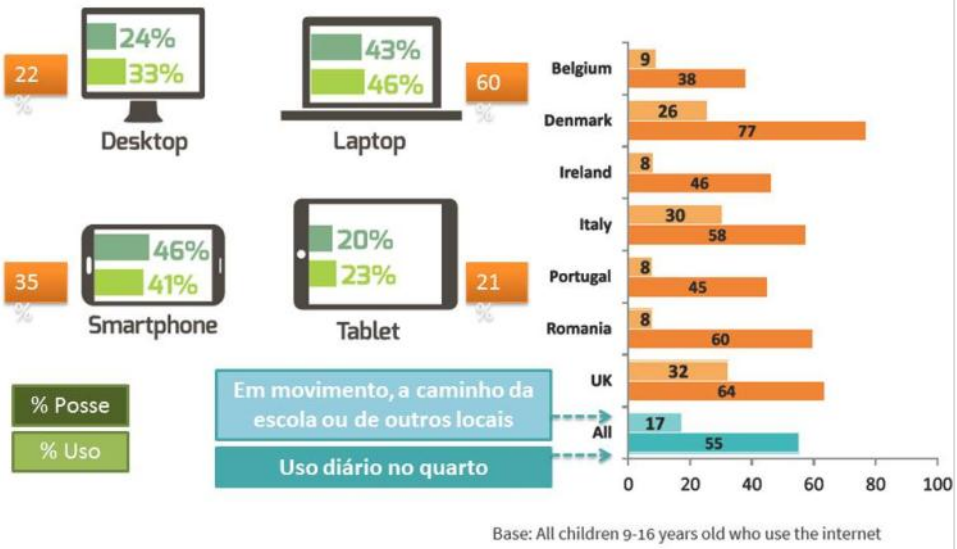
- + estudo qualitativo: **Alemanha** e **Espanha**

Net Children Go Mobile

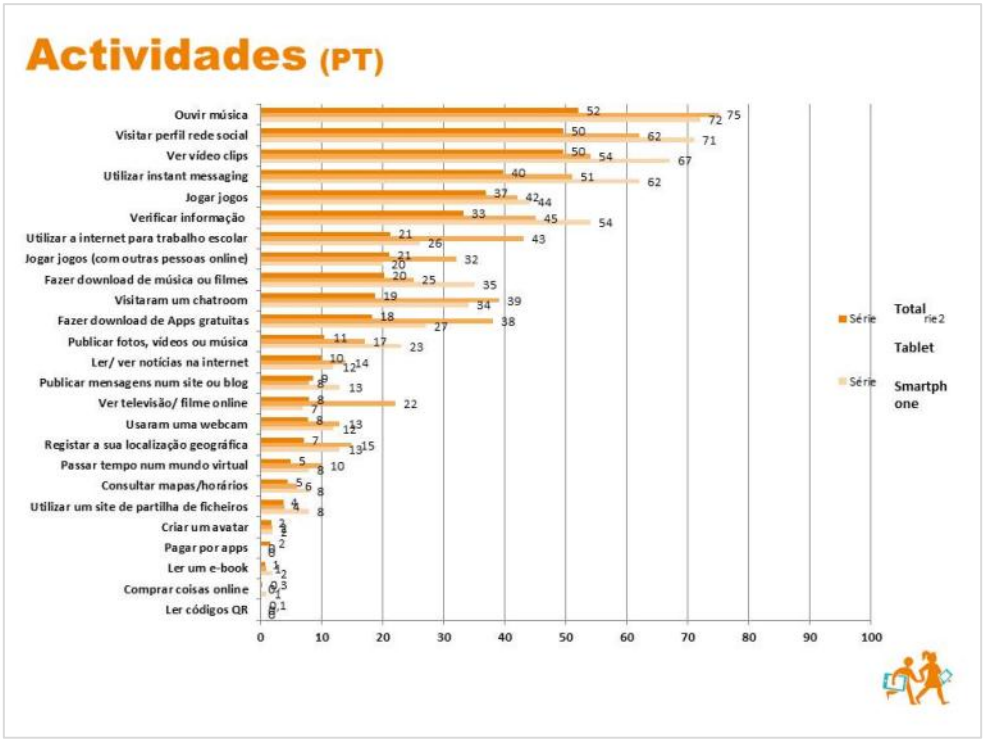
Alguns resultados para reflexão…

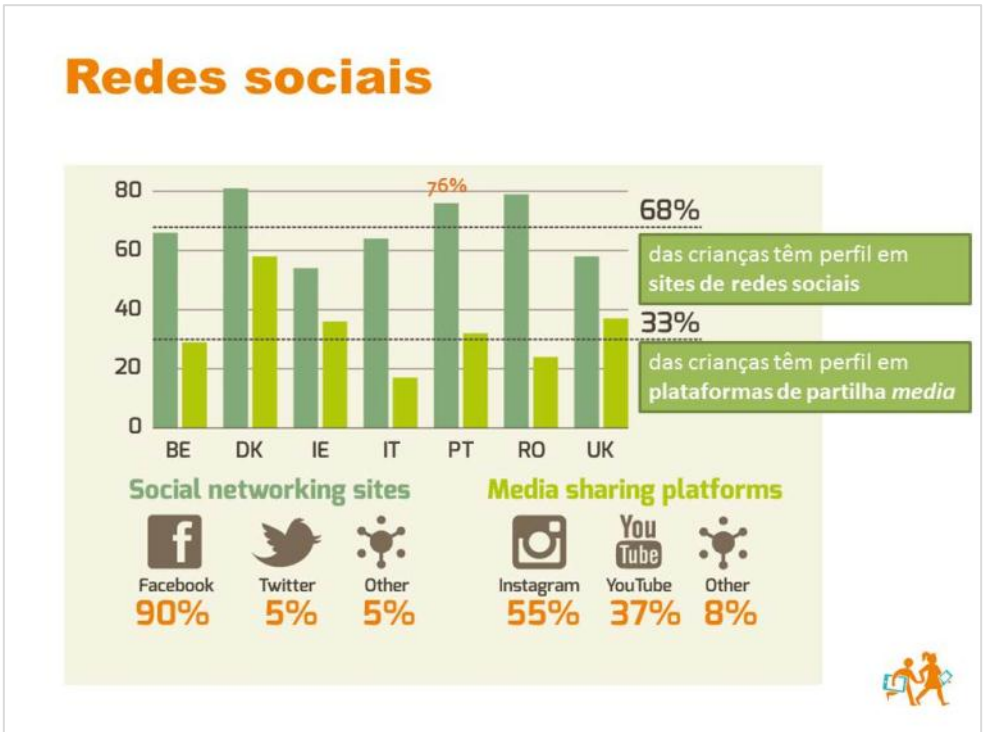
Net Children Go Mobile

Acesso e uso

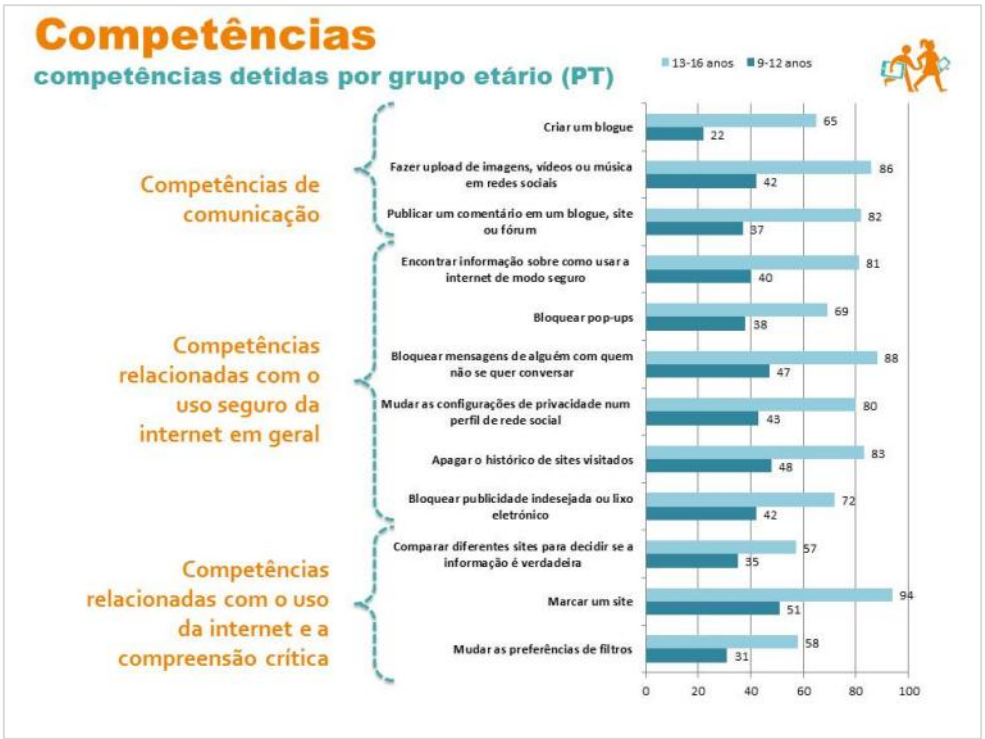


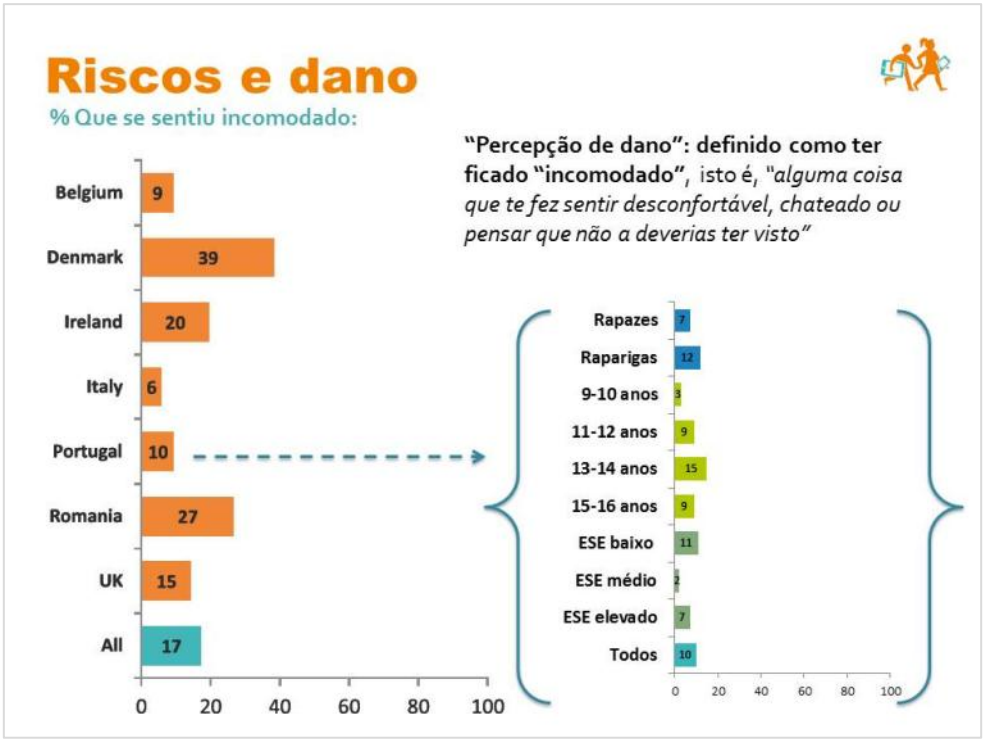
Base: All children 9-16 years old who use the internet

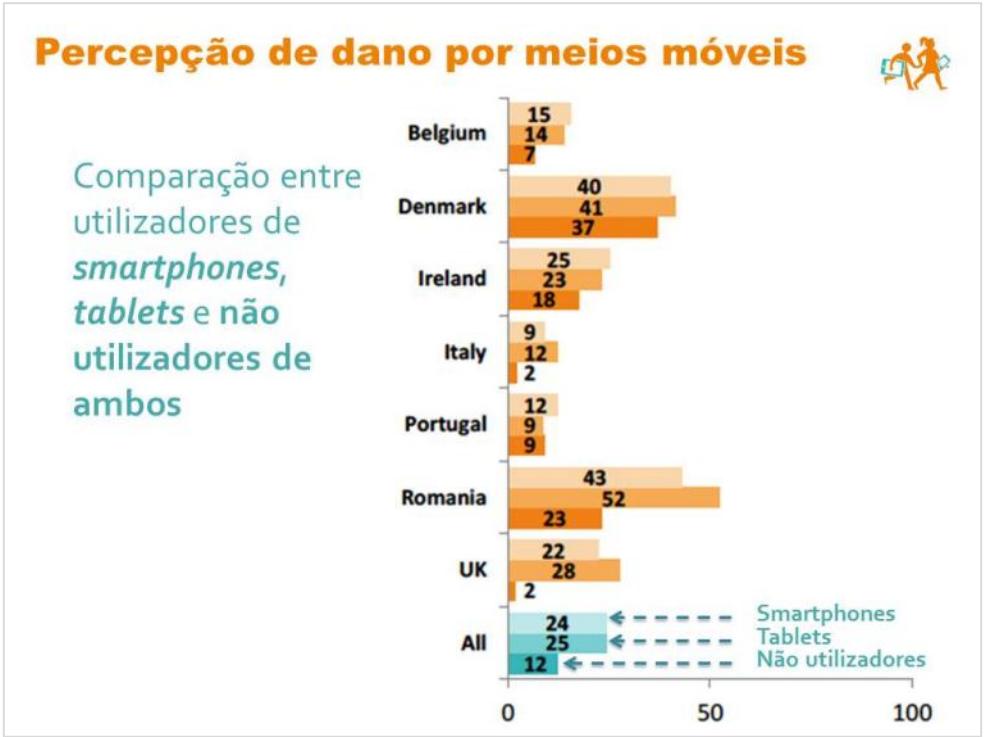

Actividades (PT)
Ouvir música
Visitar perfil rede social
Ver vídeo clips
Utilizar instant messaging
Jogar jogos
Verificar informação
Utilizar a internet para trabalho escolar
Jogar jogos (com outras pessoas online)
Fazer download de música ou filmes
Visitaram um chatroom
Fazer download de Apps gratuitas
Publicar fotos, vídeos ou música
Ler/ ver notícias na internet
Publicar mensagens num site ou blog
Ver televisão/ filme online
Usaram uma webcam
Registar a sua localização geográfica
Passar tempo num mundo virtual
Consultar mapas/horários
Utilizar um site de partilha de ficheiros
Criar um avatar
Pagar por apps
Ler um e-book
Comprar coisas online
Ler códigos QR
0 10 20 30 40 50 60 70 80 90 100
Total
Tablet
Smartphone

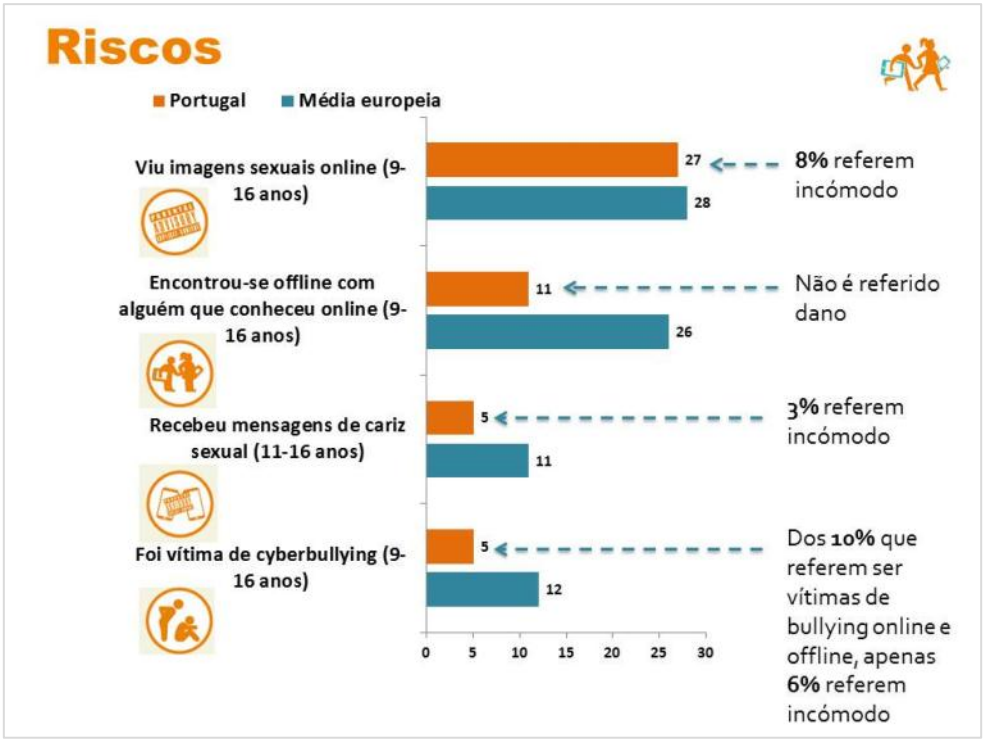

Redes sociais
80
60
40
20
0
76%
68%
das crianças têm perfil em sites de redes sociais
33%
das crianças têm perfil em plataformas de partilha media
BE DK IE IT PT RO UK
Social networking sites
Facebook 90%
Twitter 5%
Other 5%
Media sharing platforms
Instagram 55%
YouTube 37%
Other 8%

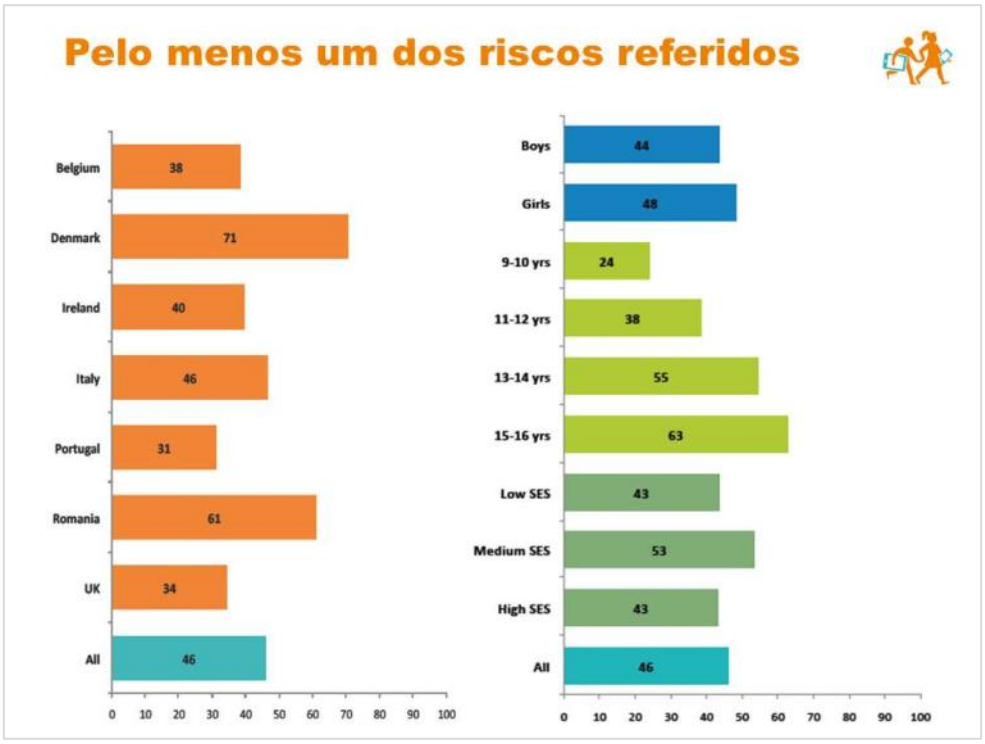

Competências
Nº de competências detidas:
Portugal
Rapazes 7,3
Raparigas 6,8
9-10 anos 1,8
11-12 anos 6,8
13-14 anos 8,2
15-16 anos 10,3
ESE baixo 7,2
ESE médio 6,3
ESE alto 7,0
Todos 7,1
0 2 4 6 8 10 12
Média europeia
8/12 Smartphone users
6,8/12 Tablet users
4,2/12 Non mobile users
5,9/12 All
Nº de competências smartphones:
How many smartphone specific skills do children believe they have?
3,9/11 9-10 years old
6,4/11 11-12 years old
8,1/11 13-14 years old
8,9/11 15-16 years old

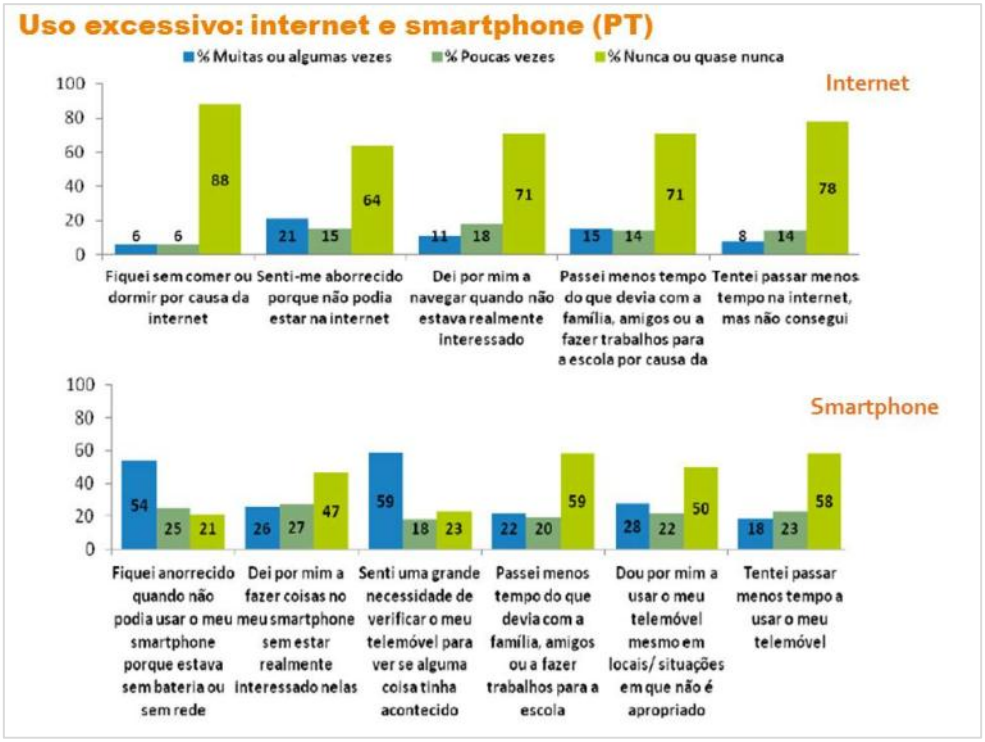

Competências
competências detidas por grupo etário (PT)
13-16 anos
9-12 anos
Competências de comunicação
Criar um blogue 65 22
Fazer upload de imagens, vídeos ou música em redes sociais 86 42
Publicar um comentário em um blogue, site ou fórum 82 37
Competências relacionadas com o uso seguro da internet em geral
Encontrar informação sobre como usar a internet de modo seguro 81 40
Bloquear pop-ups 69 38
Bloquear mensagens de alguém com quem não se quer conversar 88 47
Mudar as configurações de privacidade num perfil de rede social 80 43
Apagar o histórico de sites visitados 83 48
Bloquear publicidade indesejada ou lixo eletrónico 72 42
Competências relacionadas com o uso da internet e a compreensão crítica
Comparar diferentes sites para decidir se a informação é verdadeira 57 35
Marcar um site 94 51
Mudar as preferências de filtros 58 31
0 20 40 60 80 100

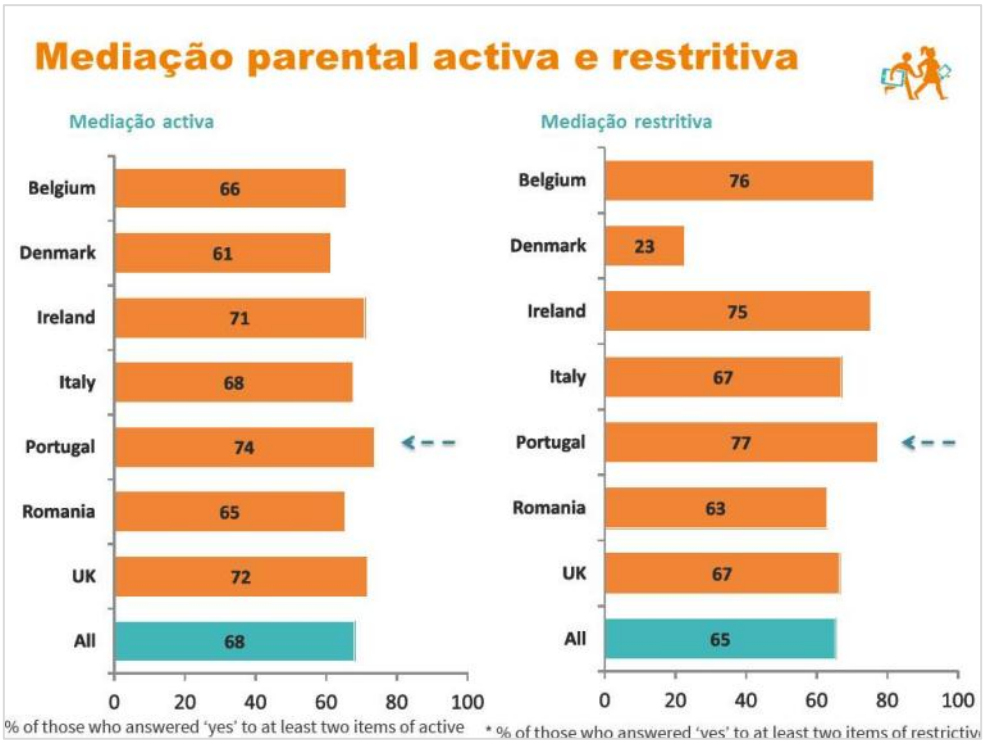

Riscos e dano
% Que se sentiu incomodado:
"Percepção de dano": definido como ter ficado "incomodado", isto é, "alguma coisa que te fez sentir desconfortável, chateado ou pensar que não a deverias ter visto"
Belgium 9
Denmark 39
Ireland 20
Italy 6
Portugal 10
Romania 27
UK 15
All 17
0 20 40 60 80 100
Rapazes 7
Raparigas 12
9-10 anos 3
11-12 anos 9
13-14 anos 15
15-16 anos 9
ESE baixo 11
ESE médio 3
ESE elevado 7
Todos 10
0 20 40 60 80 100


Percepção de dano por meios móveis
Comparação entre utilizadores de smartphones, tablets e não utilizadores de ambos
Belgium 15 14 7
Denmark 40 41 37
Ireland 25 23 18
Italy 9 12 2
Portugal 12 9 9
Romania 43 52 23
UK 22 28 2
All 24 25 12
Smartphones
Tablets
Não utilizadores
0 50 100

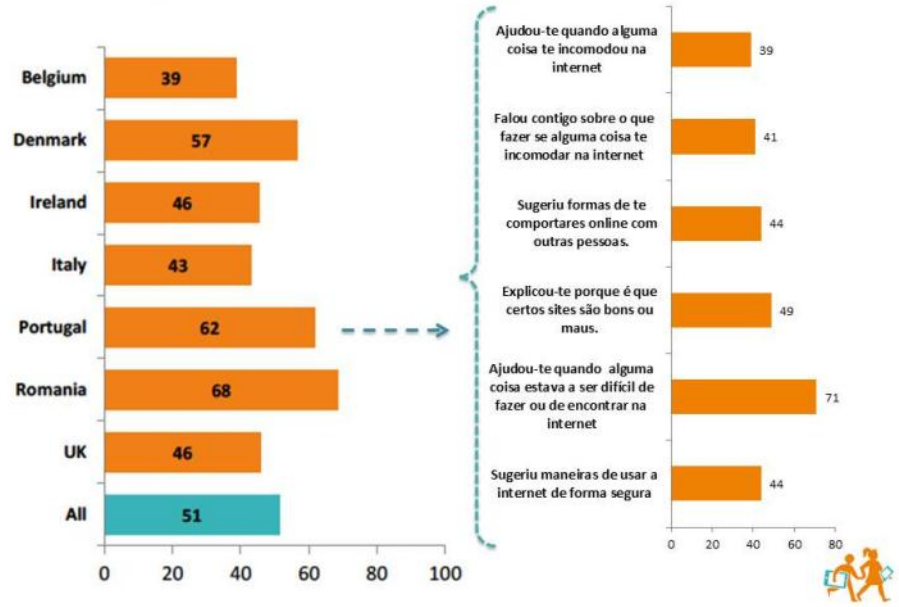

Riscos
Portugal
Média europeia
Viu imagens sexuais online (9-16 anos)
27
28
8% referem incómodo
Encontrou-se offline com alguém que conheceu online (9-16 anos)
11
26
Não é referido dano
Recebeu mensagens de cariz sexual (11-16 anos)
5
11
3% referem incómodo
Foi vítima de cyberbullying (9-16 anos)
5
12
Dos 10% que referem ser vítimas de bullying online e offline, apenas 6% referem incómodo
0 5 10 15 20 25 30


Pelo menos um dos riscos referidos
Belgium 38
Denmark 71
Ireland 40
Italy 46
Portugal 31
Romania 61
UK 34
All 46
0 10 20 30 40 50 60 70 80 90 100
Boys 44
Girls 48
9-10 yrs 24
11-12 yrs 38
13-14 yrs 55
15-16 yrs 63
Low SES 43
Medium SES 53
High SES 43
All 46
0 10 20 30 40 50 60 70 80 90 100


Uso excessivo: internet e smartphone (PT)
% Muitas ou algumas vezes
% Poucas vezes
% Nunca ou quase nunca
Internet
100
80
60
40
20
0
6 6 88
21 15 64
11 18 71
15 14 71
8 14 78
Fiquei sem comer ou dormir por causa da internet
Senti-me aborrecido porque não podia estar na internet
Dei por mim a navegar quando não estava realmente interessado
Passei menos tempo do que devia com a família, amigos ou a fazer trabalhos para a escola por causa da
Tentei passar menos tempo na internet, mas não consegui
Smartphone
100
80
60
40
20
0
54 25 21
26 27 47
59 18 23
22 20 59
28 22 50
18 23 58
Fiquei anorrecido quando não podia usar o meu smartphone porque estava sem bateria ou sem rede
Dei por mim a fazer coisas no meu smartphone sem estar realmente interessado nelas
Senti uma grande necessidade de verificar o meu telemóvel para ver se alguma coisa tinha acontecido
Passei menos tempo do que devia com a família, amigos ou a fazer trabalhos para a escola
Dou por mim a usar o meu telemóvel mesmo em locais/ situações em que não é apropriado
Tentei passar menos tempo a usar o meu telemóvel

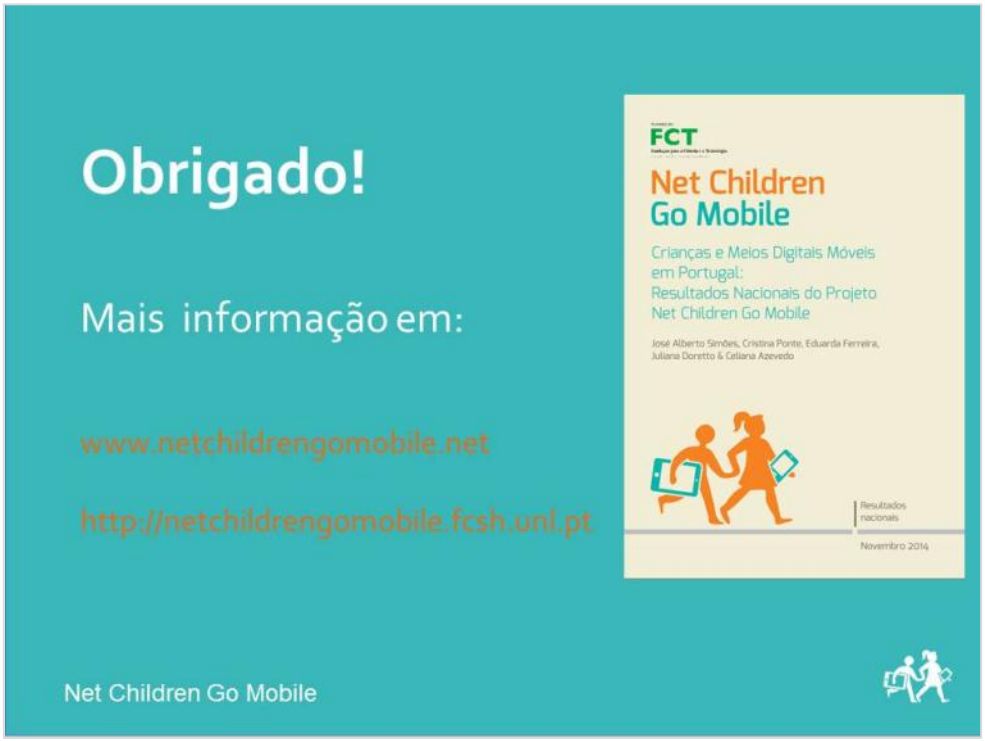

Mediação parental activa e restritiva
Mediação activa
Belgium 66
Denmark 61
Ireland 71
Italy 68
Portugal 74
Romania 65
UK 72
All 68
0 20 40 60 80 100
% of those who answered 'yes' to at least two items of active
Mediação restritiva
Belgium 76
Denmark 23
Ireland 75
Italy 67
Portugal 77
Romania 63
UK 67
All 65
0 20 40 60 80 100
* % of those who answered 'yes' to at least two items of restrictiv

Mediação activa dos pares



Pontos para reflexão

- Desafios colocados à **investigação**: como captar práticas de utilização de meios digitais por crianças e jovens num **contexto múltiplo em mudança**?
- Desafios colocados à **'sociedade'**: como garantir **bem estar** das crianças e jovens, assegurar **direitos** (de inclusão e participação digital) e promover **protecção** contra eventuais riscos (e danos)?;
- Desafios colocados aos **utilizadores**: como potenciar **oportunidades** e lidar com **riscos** e **dano**, assegurando um uso seguro da internet e de meios digitais?
- Que desafios se colocam à **mediação** dos usos destes meios digitais nas **famílias** num contexto caracterizado pela convergência mediática, mobilidade e uso individualizado?
- Que desafios se colocam às **indústrias dos *media*** – entre as **inovações tecnológicas**, os **interesses do mercado** e a **regulação** a que se encontram sujeitas?
- Que desafios se colocam aos **decisores políticos** – entre as necessidades de definir **políticas públicas** e **enquadrar juridicamente** práticas caracterizadas pela mudança?



Vídeo da apresentação

➔ https://educast.fccn.pt/vod/clips/bfomivuxs/flash.html?locale=pt

3.

A Internet e as crianças – riscos e potencialidades

Ivone Patrão

CENTRO
DE ESTUDOS
JUDICIÁRIOS

A INTERNET E AS CRIANÇAS - RISCOS E POTENCIALIDADES

Ivone Patrão*

Vídeo da apresentação

➔ https://educast.fccn.pt/vod/clips/2cbfxkcjo4/flash.html?locale=pt

* Psicóloga clínica, ISPA.

CENTRO
DE ESTUDOS
JUDICIÁRIOS

4.

A Internet e as crianças – riscos e potencialidades

Tito de Morais

CENTRO
DE ESTUDOS
JUDICIÁRIOS

A INTERNET E AS CRIANÇAS – RISCOS E POTENCIALIDADES

Tito de Morais*

Vídeo da apresentação

➔ https://educast.fccn.pt/vod/clips/qmvuzm0xn/flash.html?locale=pt

* Fundador de "MiudosSegurosNa.Net" e editor da única newsletter portuguesa sobre a segurança online de crianças e jovens.

CENTRO
DE ESTUDOS
JUDICIÁRIOS

Título:
A Internet e as crianças – riscos e potencialidades

Ano de Publicação: 2018

ISBN: 978-989-8908-23-0

Série: Formação Contínua

Edição: Centro de Estudos Judiciários

Largo do Limoeiro

1149-048 Lisboa

cej@mail.cej.mj.pt