WePROTECT GLOBAL ALLIANCE

Avaliação Mundial da Ameaça 2019

Colaborando para acabar com a exploração sexual de crianças online

AVISO:
Este documento inclui estudos de casos que podem ferir as susceptibilidades de alguns leitores. Não é adequado para crianças. Aconselhamos discrição de leitores.

PA

Agradecimentos

A Aliança Global WePROTECT gostaria de agradecer às seguintes organizações pelo aconselhamento especializado, e ao PA Consulting Group pela investigação e preparação deste relatório:

Aarambh Foundation (Índia)
ECPAT International
Comissária de e-Segurança (Austrália)
Comissão Europeia
Europol
Missão de Justiça Internacional (International Justice Mission)
Fundação de Observação da Internet (Internet Watch Foundation)
INTERPOL
Centro Nacional para as Crianças Exploradas e Desaparecidas (EUA) (National Center for Missing and Exploited Children - USA)
Agência Nacional de Investigação Criminal (Reino Unido) (National Crime Agency - UK)
Parceria Global para o Fim da Violência Contra Crianças (The Global Partnership to End Violence Against Children)
A Fundação Lucy Faithfull
UNICEF Gana
Departmento de Justiça dos EUA

Conteúdo

01 Prefácio

por Ernie Allen, Presidente da Aliança Global WePROTECT

Na nossa última Cimeira, co-organizada com a Parceria Global para o Fim da Violência Contra Crianças e com o governo da Suécia em 2018, a Aliança Global WePROTECT publicou a nossa primeira Avaliação Mundial da Ameaça. Foi a primeira iniciativa deste género, juntando peritos de toda a Aliança para produzir uma análise global, disponível ao público, da escala e natureza da ameaça com que as crianças se deparam online, com o objectivo de reforçar a nossa resposta internacional.

Com a ajuda da PA Consulting, que apoiou a avaliação da ameaça generosamente pro bono, e com a perícia e conhecimentos dos nossos membros, fizemos mais e melhor e ouvimos os vossos comentários. Nesta nova versão da avaliação da ameaça há novas perspectivas sobre a natureza do abuso sexual de crianças online no Sul Global, e fazemos uma análise do impacto que a inovação tecnológica terá na ameaça.

As nossas conclusões são marcantes. Verificamos que a escala do problema, quer em termos absolutos, quer em termos de denúncias às forças policiais e à sociedade civil, está a aumentar a um nível alarmante. E por detrás de cada um destes casos há uma criança que precisa de ser protegida e apoiada. Este "tsunami" de casos aumenta a demanda de cada pilar da Aliança Global WePROTECT: governos, forças policiais, sociedade civil e indústria tecnológica. Com o aumento da conectividade da Internet, especialmente no Sul Global, os criminosos conseguem encontrar e explorar novas vítimas.

Ao mesmo tempo, deparamo-nos com uma redução de denúncias, onde a encriptação aplicada pela indústria de comunicações significa que as empresas de tecnologia conseguem identificar cada vez menos o uso mal-intencionado das suas próprias plataformas. E estamos a notar uma disparidade cada vez mais acentuada entre os países que tiveram tempo para desenvolver serviços de apoio sofisticados, alinhados com a sua própria evolução tecnológica, e os países que se lançam para a paridade tecnológica mais depressa do que se conseguem preparar para tal. O anonimato e a segurança da comunicação continuam a permitir que os criminosos criem espaços seguros onde podem interagir e difundir ferramentas e técnicas para facilitar a exploração. Ao mesmo tempo que damos passos para compreender as metodologias e motivações dos criminosos, e as necessidades e impactos do abuso nas vítimas, salienta-se a importância da prevenção e protecção – parar o dano antes que aconteça. As estimativas acauteladas do impacto financeiro deste crime ascendem a milhares de milhões de dólares respeitantes aos serviços de saúde, assistência social e impacto na qualidade de vida. Há razões económicas, operacionais e morais para melhorarmos a nossa resposta.

À medida que vai havendo cada vez mais crianças online por todo o mundo, e o panorama tecnológico muda e evolve, nós, mais do que nunca, precisamos de um fórum para colaborar, trocar ideias e agir. A Aliança Global WePROTECT apresenta-se como uma plataforma, uma voz, e um conjunto de instrumentos para que os seus associados possam agir contra o abuso sexual de crianças online à escala mundial. Paralelamente a esta avaliação da ameaça lançamos também a Resposta Estratégica Global, a qual oferece um quadro de acção a um nível transnacional, baseada em opiniões de peritos. Continuaremos a lutar para consciencializar, apoiar acções, e, em última análise, acabar com a exploração sexual de crianças online.

Ernie Allen
Presidente, Conselho de Administração da Aliança Global WePROTECT

Definições e missão

A Aliança Global WePROTECT (AGWP) é uma iniciativa internacional dedicada à acção nacional e mundial para acabar com a exploração sexual de crianças online (Online Child Sexual Exploitation – OCSE). Neste relatório adoptámos os seguintes termos e abreviações:

CSEA: Abuso e Exploração Sexual de Crianças (*Child Sexual Exploitation and Abuse*), também chamado de CSAE e CSE por algumas organizações, é uma forma de abuso que ocorre quando um indivíduo ou grupo se aproveita de um desequilíbrio de poder para coagir, manipular, ou enganar uma criança ou jovem com menos de 18 anos a praticar actividades sexuais.

A vítima pode ter sido explorada sexualmente mesmo quando a actividade sexual aparenta ser consensual. A exploração sexual de crianças nem sempre envolve contacto físico: pode ser praticada através do uso de tecnologia.[1]

A AGWP aprova o âmbito descrito na Convenção Europeia para a protecção de Crianças contra a Exploração e Abuso Sexual, conhecida como a "convenção de Lanzarote", que abrange todos os crimes possíveis contra crianças, incluindo o abuso sexual de uma criança, a exploração de crianças através de prostituição, aliciamento e corrupção de crianças pela exposição a conteúdos sexuais, e actividades e crimes relacionados com material de abuso de crianças. A Convenção abrange o abuso sexual no seio da sua família, ou "círculo de confiança", além de actos praticados com fins comerciais ou de lucro. A Convenção de Lanzarote apresenta os seguintes seis crimes sexuais:

- Artigo 18º: Abusos sexuais
- Artigo 19º: Prostituição de menores
- Artigo 20º: Pornografia de menores* [considerada neste relatório como Material de Abuso Sexual de Crianças (*Child Sexual Abuse Material* – CSAM)]
- Artigo 21º: Participação de uma criança em espectáculos pornográficos
- Artigo 22º: Corrupção de menores
- Artigo 23º: Solicitação de crianças para fins sexuais (também conhecido como "aliciamento online" ou *online grooming*).

CSAM: Apesar de as agências da ONU e outras instituições internacionais descreverem imagens e vídeos indecentes de crianças como "pornografia de menores", depois do Projecto Interagência de Semântica e Terminologia finalizado em Junho de 2016, a WPGA mantém que a terminologia "material de abuso sexual de crianças" (*child sexual abuse material* – CSAM) representa com maior precisão a natureza hedionda da exploração e violência sexual de crianças protegendo, simultaneamente, a dignidade das vítimas.

Norte Global e Sul Global:
De forma a distinguir entre os níveis diferentes de desenvolvimento entre os países-membros, neste relatório usamos o termo "Norte Global" para indicar os países do G8, os Estados Unidos da América, todos os estados da União Europeia, Israel, Japão, Singapura, Coreia do Sul, Austrália, Nova Zelândia, e quatro dos cinco membros permanentes do Conselho de Segurança das Nações Unidas, excluindo a China. O "Sul Global" inclui a África, a América Latina, o Médio Oriente e a Ásia em desenvolvimento. Inclui três das economias recentemente avançadas dos países do BRIC (excluindo a Rússia), que são o Brasil, a Índia, e a China.

Neste relatório usamos os termos "criminoso" e "autor do crime" indiferentemente para indicar aqueles que praticam exploração e abuso sexual de crianças online.

Usamos também os seguintes termos para definir os tipos de alojamento de serviços online:

- a **Internet Visível** é a parte da internet facilmente disponível ao público geral e onde se podem realizar buscas com motores de busca normais.
- a **web profunda** (*Deep Web* em inglês) é a parte da Internet onde o conteúdo não está indexado pelos motores de busca normais, e inclui muitos usos normais, como webmail, plataformas de bancos online, e serviços por assinatura. O conteúdo pode ser localizado e acedido por um URL ou IP directo, e pode requerer palavra-passe ou outros meios de segurança após a página de acesso público.
- a **web escura** (também conhecida como *Dark Net* e *Dark Web* em inglês) é um termo contestado, mas compreendido por quase todas as autoridades, e, neste relatório, entende-se como uma camada de informação e páginas apenas acessíveis através das chamadas "redes sobrepostas", tais como as Redes Privadas Virtuais (ou *Virtual Private Network* – VPN) e as redes de partilha de ficheiros *peer-to-peer* (P2P), as quais bloqueiam o acesso público. Os utilizadores precisam de software especial para aceder à web escura porque a maior parte está encriptada, e a maior parte das páginas na web escura são alojadas anonimamente.

02 Objectivos da Avaliação Mundial da Ameaça

A primeira Avaliação Mundial da Ameaça (*Global Threat Assessment* – GTA) foi publicada em Fevereiro de 2018 e foi anunciada na Agenda 2030 para as Crianças (*2030 Agenda for Children*): Soluções para Acabar com a Violência, em Estocolmo, na Suécia. Foi o primeiro relatório deste género – uma visão global e abrangente das mudanças tecnológicas, vulnerabilidade das vítimas, comportamento dos criminosos, e o ponto de intersecção onde a exploração e abuso sexual de crianças (*child sexual exploitation and abuse* – CSEA) tem maior incidência.

A conclusão central da GTA18 foi de que "a tecnologia está a permitir níveis de organização sem precedentes às comunidades de autores do crime, o que, por sua vez, cria ameaças novas e persistentes à medida que estes indivíduos e grupos exploram "portos de abrigo" e acesso às vítimas "a pedido"".[2]

Estas descobertas fundamentadas em dados concretos serviram como um apelo à mobilização de governos nacionais para redobrar os esforços e encontrar formas novas e inovadoras de combater esta ameaça aos mais vulneráveis das nossas sociedades. Os governos nacionais responderam disponibilizando capacidades de partilha de informações para destabilizar as comunidades criminosas mais perigosas, melhorando os recursos educativos e de apoio, e implementando novas medidas legislativas e regulamentares que contribuem para um melhor entendimento das empresas de tecnologia, e clarificam a sua responsabilidade em manter as crianças seguras online através acções robustas para combater conteúdos e actividades ilegais.

90 actuais países membros da Aliança Global WePROTECT

22 dos nomes mais importantes da indústria mundial de tecnologia

26 organizações internacionais e não-governamentais líderes

O relatório deste ano foi encomendado com o apoio e a peritagem dos membros do Conselho de Administração da Aliança Global WePROTECT, e pretende avançar a partir do amplo sucesso e impacto do GTA18. O seu objectivo é demonstrar a natureza, escala, e complexidade da exploração sexual de crianças online (online child sexual exploitation – OCSE), de forma a apoiar uma mobilização significativa – levando os estados-nação, as empresas mundiais de tecnologia e o sector terciário a encontrar novas maneiras de colaborar para combater esta ameaça de rápido desenvolvimento. O Modelo de Resposta Nacional da WePROTECT oferece diretrizes e apoio a países e organizações, para os ajudar a formular a sua resposta ao OCSE.

A avaliação opera pela mesma perspectiva do GTA18 e mantém os mesmos objectivos, como indicados abaixo, incidindo numa compreensão mais aprofundada de cada tema. Procurámos oferecer uma perspectiva mais global da ameaça, considerando as diferenças de contexto e perspectivas culturais para além dos dados predominantemente da América do Norte e Europa Ocidental, e dos estudos de caso usados no nosso primeiro relatório. O presente relatório procura:

- fomentar a consciencialização e compreensão da OCSE
- oferecer uma melhor compreensão da ameaça e de como está a evoluir
- permitir uma melhor compreensão do impacto nas vítimas e de um impacto societal mais alargado
- criar marcos de referência em relação ao GTA18 para avaliar as mudanças da natureza e escala da ameaça, e também do impacto positivo que as suas intervenções estejam a ter
- apresentar estudos de caso recentes para apoiar os membros, dando prioridade às intervenções e decisões de investimento individuais e colectivas.

Metodologia

O presente relatório é um meta-estudo, combinando os resultados de estudos múltiplos internacionais, num esforço para aumentar o poder e impacto dos relatórios individuais, melhorar as estimativas da escala da OCSE em termos mundiais e fazer uma avaliação quando houver uma discordância de relatórios. Esta investigação secundária é reforçada com investigação primária a partir de estudos de caso operacionais disponibilizados pelas organizações membro da WePROTECT.

Pontos de dados importantes

18,4 milhões de reencaminhamentos de material de abuso sexual de crianças por empresas de tecnologia dos EUA ao Centro Nacional de Crianças Desaparecidas e Exploradas (*National Center for Missing and Exploited Children* – NCMEC) em 2018[3]

2/3 do total de 18,4 milhões de reencaminhamentos ao NCMEC tiveram origem em serviços de mensagens, em risco de desaparecerem se for implementada a encriptação de ponta-a-ponta.[4]

13,3 milhões+ de imagens suspeitas processadas pelo Centro Canadiano para a Proteção da Criança (Projecto Aracnídeo) foram indicadas para revisão por analistas, resultando em 4,6 milhões de avisos para desactivação de imagens enviados aos fornecedores de acesso à Internet.[5]

94% do material de abuso sexual de crianças encontrado online pela Fundação de Observação da Internet (*Internet Watch Foundation* – IWF) continha imagens de crianças com idade igual ou inferior a 13 anos.

39% do material de abuso sexual de crianças encontrado online pela IWF continha imagens de crianças com idade igual ou inferior a 10 anos.[6]

46 milhões de imagens ou vídeos únicas relacionadas com CSAM no repositório da EUROPOL.[7]

750,000 indivíduos que se calcula terem a intenção de se ligarem a crianças por todo o mundo para fins sexuais online em qualquer dado momento.[8]

03 Conclusões sumárias

Tendências recentes indicam um "tsunami" de incidências de OCSE, criando cada vez mais vítimas e sobreviventes no seu percurso.

A escala, severidade, e complexidade de CSEA online cresce a um passo mais célere que as actividades e capacidade de resposta para a combater, com reencaminhamentos das empresas de tecnologia parceiras e forças policiais a atingir números sem precedente.[9] Surge aqui uma necessidade urgente de os governos, organizações de forças policiais, a indústria da tecnologia, e organizações do sector terciário colaborarem para aumentar a resposta colectiva.

Os obstáculos práticos que impedem uma colaboração, partilha, e aprendizagem internacional mais estreita são a natureza fragmentada da resposta de segurança online de cada nação, normalmente abrangendo policiamento, assistência social, regulamentação e educação.

A rápida proliferação mundial de posse de dispositivos móveis e acesso à Internet está a criar uma assimetria entre o Norte e o Sul Global. Todas as nações enfrentam o mesmo desafio da evolução rápida da tecnologia, mas a entrada para o mundo digital difere entre as sociedades que adoptaram os serviços da internet progressivamente enquanto aprendem a proteger as suas infraestruturas e cidadãos online, e aquelas que recebem o produto final instantaneamente, sem tempo para desenvolver e evoluir os seus serviços educacionais e de apoio, forças policiais e resposta regulamentar. A cadeia de resposta é apenas tão forte quanto o seu elo mais fraco. Nas palavras de um investigador da INTERPOL:

> "A diferença equipara-se a entrar numa piscina com cautela, na zona menos funda, com o equipamento e educação para aprender a nadar, e a lançar-se na piscina na parte funda para aprender a nadar. [10]"

A crescente disponibilidade de ferramentas avançadas de anonimização e encriptação e a partilha de ficheiros através de redes *peer-to-peer* (P2P) com encriptação ponta-a-ponta proporcionam aos criminosos um acesso mais fácil e mais seguro a crianças vulneráveis, e a manter redes de pessoas que partilham um interesse sexual em crianças. Há indícios de uma ligação entre a filiação em larga escala nestes "portos de abrigo" online (a Agência Nacional de Crime do Reino Unido identificou 2,88 milhões de contas filiadas nos dez sites mais nocivos da web escura) e a crescente comodificação e industrialização de material de abuso sexual de crianças (CSAM).[11]

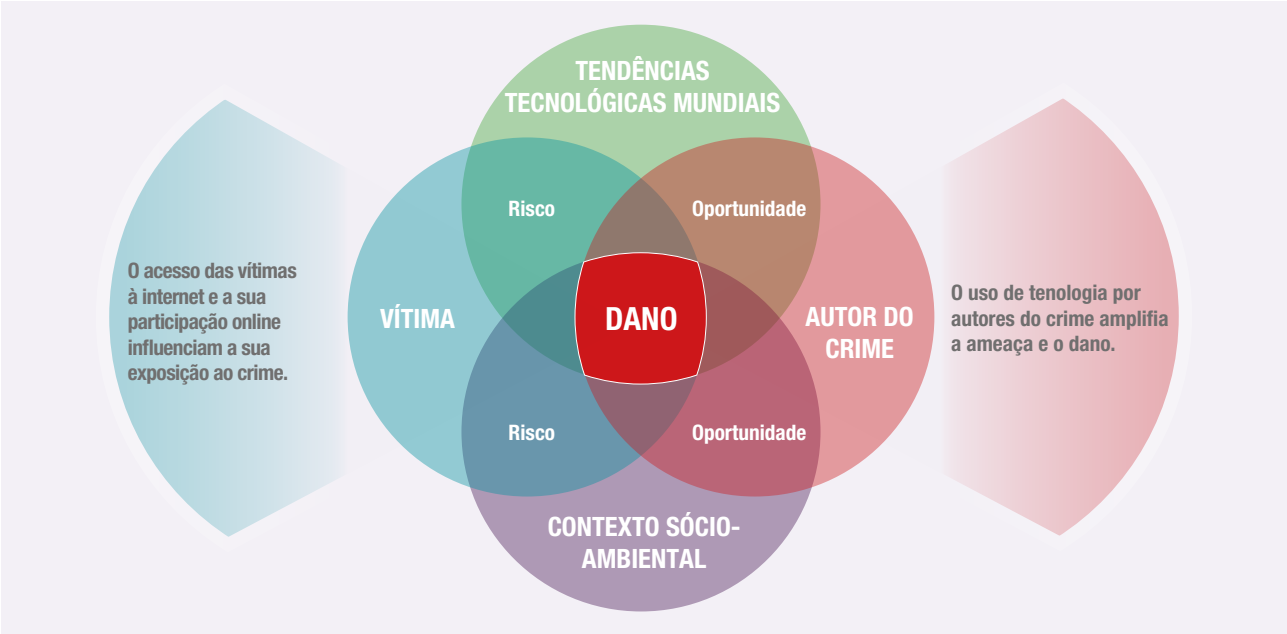
Concomitantemente, o aumento de posse de dispositivos e acesso de crianças à internet sem supervisão aumenta a sua exposição ao risco de exploração e abuso online. O seu nível de maturidade, compreensão limitada dos riscos de estar online, e a mudança das atitudes relacionadas com comportamento online agravam a situação, onde um em cada quatro adolescentes recebe e-mails e mensagens SMS sexualmente explícitas, e onde um em cada sete as envia.[12]

Há uma esfera crescente de dano onde a proliferação online de imagens e vídeos indecentes de crianças está a superar rapidamente a capacidade das organizações responsáveis pela identificação proactiva e remoção deste material. Os seguintes capítulos apresentam provas de que estas ameaças e desafios continuarão a crescer sem uma acção decisiva e colectiva.

A Avaliação Mundial de Ameaça do ano passado identificou a convergência maliciosa de quatro elementos com a maior influência na esfera de dano e que ajudam a explicar o aumento do CSEA online:

- as tendências tecnológicas mundiais;
- as alterações do comportamento dos criminosos;
- a exposição online das vítimas;
- o contexto socio-ambiental.

Figura 1: Quatro perspectivas criam a esfera de dano: tecnologia, criminosos, vítimas, e factores socio-ambientais.



Novas investigações pelo mundo e novos estudos de caso validam as nossas conclusões anteriores e destacam novos factores que contribuem para uma esfera de dano em expansão. No seu conjunto, estes novos dados indicam um tsunami de aumento de CSEA online, e um aumento igual de potenciais vítimas que precisam de ser protegidas, e sobreviventes que precisam de apoios adequados.

Apresentamos um resumo das quatro perspectivas analisadas neste relatório e na Figura 1 infra.

1. Tendências da tecnologia no mundo: a industrialização de serviços online seguros

A GTA18 destacou a emergência de comunidades de criminosos a usar os serviços da web escura para partilhar imagens e dicas de aliciamento de crianças e para evitar detecção.[13] Estas tendências continuam e são ampliadas pela industrialização de serviços Web de superfície de fácil acesso e prontos para o consumidor, que permitem uma maior privacidade, segurança e anonimato. Incluem redes de partilha de ficheiros P2P seguras, serviços de alojamento que disfarçam CSAM nos sites da internet normal, e serviços de pagamento móvel e de envio de mensagens que contornam a necessidade de registo e identificação.

2. Comportamento dos criminosos: o ciclo vicioso

A forma como compreendemos o percurso dos criminosos precisa de uma análise mais aprofundada e mais estudos académicos. Nem todos os criminosos tendem a usar fóruns de internet; nem todos os que vêm CSAM online irão manipular ou coagir crianças para actividades sexualmente explícitas; e nem todos os criminosos que encomendam transmissão ao vivo de abuso “a pedido” irão escalar o seu comportamento a abusar directamente uma criança. O abuso online, através da distância física da vítima, pode aguçar o risco de desvio comportamental, e há indícios de que os que se juntam a “grupos de interesse especial” online são encorajados para mais violência e crianças mais jovens numa busca de estatuto pessoal no seio da sua comunidade de criminosos.[14]

3. Vulnerabilidade das vítimas: normalização de comportamento online de risco

Os jovens estão cada vez mais vulneráveis a interacções maliciosas resultantes da redução constante da idade com que têm acesso a dispositivos, às redes sociais e jogos online sem supervisão. Uma tendência preocupante é a normalização do comportamento sexual online, com um grande número de crianças (com idades cada vez mais novas) a partilhar imagens indecentes autogeradas (*self-generated indecent images* – SGII), quer através de decepção e coação, actividade online consensual com outra criança de uma idade apropriada, ou para afirmação social. Aumenta, assim, a quantidade de material disponível aos criminosos e a vulnerabilidade das crianças à exploração e abuso por adultos, além de intimidação online (*cyberbullying*) por outras crianças. Há casos de fraudes e criminosos organizados que concentram os seus esforços em crianças para adquirir imagens e vídeos sexualizados, e de criminosos por contacto que partilham CSAM de forma mais rápida e abrangente.[15]

4. O contexto socio-ambiental: o salto para a paridade tecnológica

Nos 12 meses anteriores a Janeiro de 2019, houve 367 milhões de novos utilizadores de Internet no mundo, dos quais a INTERPOL calcula que 1,8 milhões sejam homens com um interesse sexual em crianças agora online (notando-se, contudo, que nem todos se tornam em criminosos sexuais).[16]A entrada no mundo digital varia entre as comunidades que adoptaram a internet progressivamente e aquelas que se lançam numa paridade tecnológica, recebendo a gama completa dos serviços de Internet instantaneamente e sem um período para desenvolver estruturas educativas e apoio, e uma capacidade de resposta regulamentar e forças policiais capazes de lidar com esse crescimento. É de notar que, desde a GTA18, o trabalho e influência mundial da Comissão para Banda Larga para o Desenvolvimento Sustentável tem dado maior ênfase na OCSE.[17]

Crescimento desde a GTA18

367 milhões de novos utilizadores de Internet (um crescimento de 9%)[18]

122 milhões mais crianças online, com base em estimativas da UNICEF de que 1 em cada 3 utilizadores de Internet é uma criança[19]

80% de aumento de denúncias relacionadas com CSAM enviados à rede mundial de linhas de apoio da INHOPE[20]

100% de aumento do número de fotografias de crianças a ser abusadas sexualmente denunciadas pelas empresas de tecnologia[21]

33% de aumento de URLs onde CSAM removido pela Fundação de Observação da Internet.[22]

04 Tendências de tecnologia

O aumento do acesso online, novas tecnologias, e o crescimento de "encriptação de origem" estão a contribuir para o crescimento de incidentes

O número de dispositivos móveis e utilizadores de Internet continua a crescer. Hoje em dia há no mundo mais de cinco mil milhões de utilizadores únicos de telemóvel e mais de quatro mil milhões de utilizadores de Internet, representando um crescimento respectivo de 2% e 9% desde 2018. Houve também um crescimento de 9% no número de utilizadores de redes sociais, ascendendo a 3,5 mil milhões.[23]

O aumento do acesso à Internet móvel está a facilitar um maior acesso a jogos online, pagamentos electrónicos, comércio electrónico, e a Internet das Coisas (IdC), equipamentos como monitores de bebés, brinquedos ligados à Internet e equipamentos com câmara web. Estes produtos estão cada vez mais baratos e com um tempo de vida mais longo, com o acesso mais fácil a equipamentos em segunda mão por consumidores de renda baixa em nações em desenvolvimento.

Estes desenvolvimentos estão a permitir que o Sul Global atinja paridade tecnológica com o Norte Global. Enquanto que o Norte tem tido uma evolução relativamente moderada no acesso dos agregados familiares à Internet e tecnologias móveis durante as duas últimas décadas, as nações do Sul estão a passar rapidamente de um acesso limitado à internet a serviços de Internet fiáveis e de alta velocidade, e a redes móveis de 4G e 5G, contornando a necessidade de estabelecer uma infraestrutura dispendiosa de linha fixa e Internet de banda larga.

O número de utilizadores absolutos na Índia cresceu em cerca de 100 milhões (21%) desde o ano passado. Quanto ao crescimento da Internet relativo ao tamanho da população, oito dos 10 países com maior crescimento foram países africanos. O Djibouti, a Tanzânia, o Niger e o Afganistão aumentaram o dobro cada um o número de utilizadores de Internet em relação ao ano passado. Aliás, entre os 20 países com o maior aumento relativo de internet no último ano, 19 eram países doi Sul Global.[24]

O Modelo de Resposta Nacional da WePROTECT oferece um contexto valioso a estas nações para avaliarem as suas capacidades de combate ao OCSE.

Calcula-se que 1,8 milhões de novos utilizadores de Internet masculinos no último ano tenham um interesse sexual em crianças.

Uma consequência deste crescimento rápido de equipamentos e acesso à Internet é o crescimento proporcional do número de adultos com interesses sexuais em crianças que estão agora online, e do número de crianças em risco de exposição a estes indivíduos devido a interacções online sem supervisão.

Figura 2: Crescimento digital Jan 2018 – Jan 2019[25]

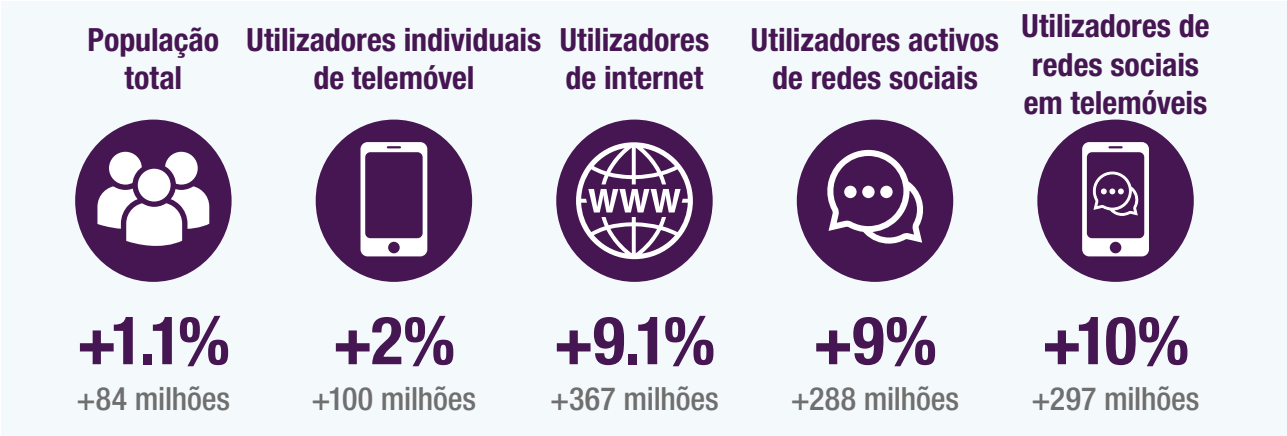
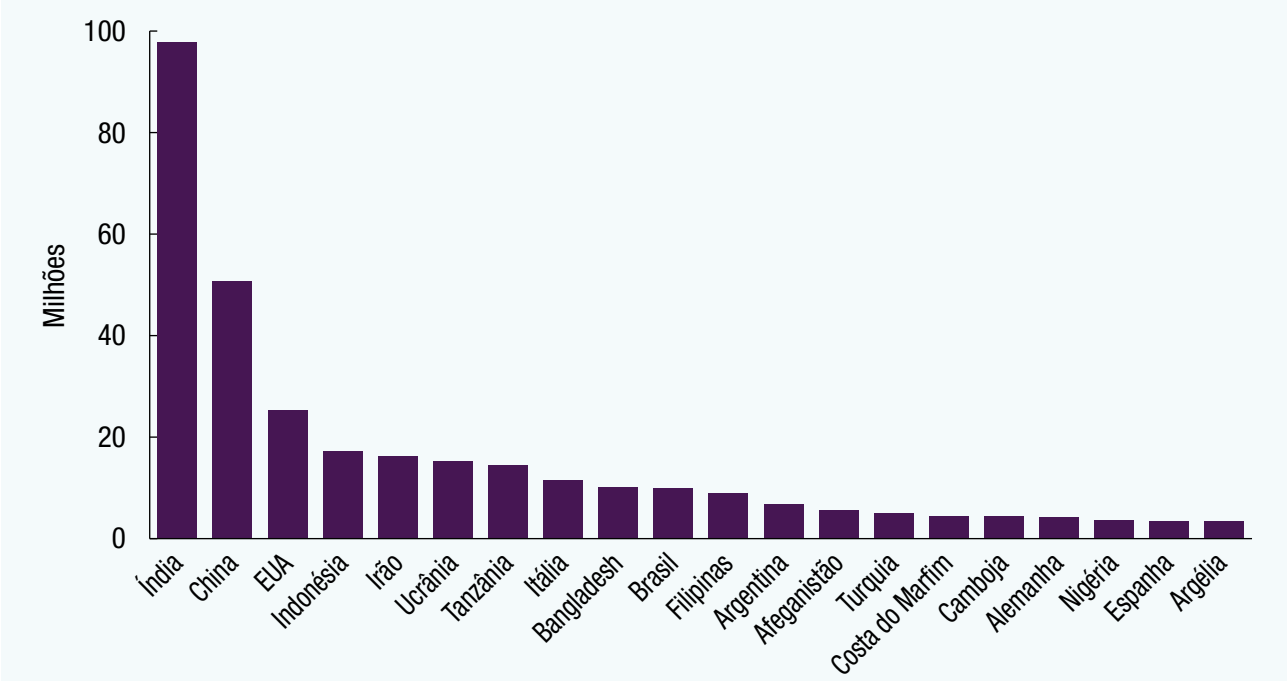


Figura 3: 20 países com a maior taxa de crescimento de uso absoluto de Internet (2018-19)



Com base em estudos académicos de que 1% da população masculina está predisposta a um interesse sexual em crianças pré-pubescentes, a INTERPOL calcula que é provável que haja aproximadamente mais 1,8 milhões de homens nesta categoria a usar a Internet agora, quando comparado com o ano passado (assumindo uma adopção do acesso à Internet à razão de homens e mulheres de 50:50).[26]Trata-se de uma estimativa modesta, uma vez que o 1% se refere apenas a pedófilos com um interesse sexual em crianças pré-pubescentes. Noutros estudos calcula-se que entre 2,2% e 4,4% de homens adultos viram, propositadamente, CSAM de crianças pré-pubescentes online.[27]

Sendo que grande proporção do aumento de utilizadores de Internet ocorreu no Sul Global, o risco que estas "novas entradas" representam é amplificado pela falta de uma educação sobre segurança online coordenada, e serviços de forças policiais e protecção da criança menos desenvolvidos, o que significa que mais crianças se tornam vítimas dos criminosos e não recebem o apoio de medidas de segurança.

A tecnologia está a reduzir as barreiras de entrada de OCSE

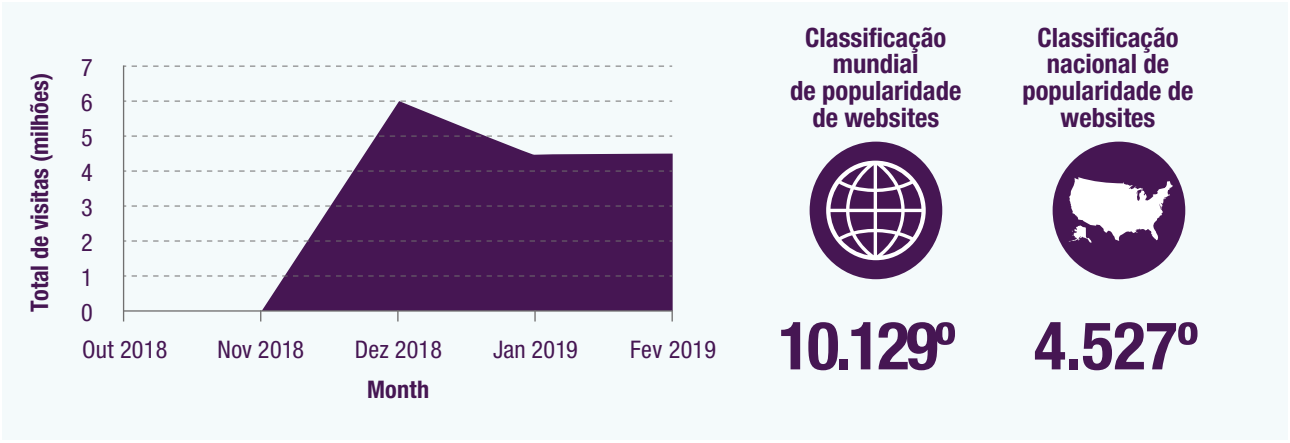
Em 2018 as empresas de tecnologia dos EUA (com utilizadores por todo o mundo) denunciaram mais de 45 milhões de fotografias e vídeos online de crianças a sofrerem abuso sexual – mais do dobro dos relatos do ano anterior.[28]

O grau de disponibilidade de CSAM é significativo, e é possível criar e aceder mais rapidamente aos sites que alojam este material do que identificá-los e fechá-los. Entre 2014 e 2018, o número de URLs de abuso sexual de crianças eliminado por ano mais do que triplicou, ascendendo de 31.226 a 105.047 em 2018. Entre 1996 e 2019 a Fundação de Observação da Internet (*Internet Watch Foundation* – IWF) eliminou quase meio milhão de páginas de Internet que exibiam abuso sexual de crianças.[29]

Um site de Internet que alojava CSAM recebeu 6,5 milhões de visitas no seu primeiro mês de operação

A INTERPOL identificou uma página na web superficial que, desde que surgiu em Novembro de 2018, recebeu 6,5 milhões de visitas no primeiro mês de operação, passando depois a uns 4,67 milhões de visitas por mês. Em Fevereiro de 2019 foi classificada como a 4.527ª página mais popular nos EUA e a 10.129ª página mais popular no mundo.[30]

Figura 4: Visão geral do tráfego de sites mais populares com alojamento de CSAM (Fevereiro de 2019)



A nossa Avaliação Mundial da Ameaça de 2018 destacou sites semelhantes na web escura com cerca de um milhão de visitas.[31]

Na web escura os criminosos podem seguir material mais restrito. Em 2018, registaram-se 2,88 milhões de contas ao longo dos dez sites de CSEA mais nocivos na web escura.[32]A web escura pode ampliar os comportamentos actuais dos criminosos, onde estes supostos "portos seguros" permitem aos criminosos conversar sobre os seus interesses sexuais com mais liberdade e partilhar imagens extremistas. Contudo, o uso da web escura e da web superficial não é binário: as autoridades canadianas indicaram vastas compilações de material encriptado e guardado em cacifos na web superficial, e os links partilhados nos fóruns da web escura.[33]

O crescimento da encriptação

Tendemos a associar a web escura como sendo um ambiente onde atributos como o anonimato, a encriptação e a segurança contra detecção são usados para esconder actividade criminosa. Por outro lado, é comum pensarmos na web superficial como proporcionando um acesso fácil e disponibilidade geral de serviços normais ao consumidor. Contudo, o impacto da encriptação ponta-a-ponta de sites normais populares de redes sociais e de serviços de envio de mensagens, considerados juntamente com um processo de registro fraco e com o uso de Redes Privadas Virtuais (*Virtual Private Networks* – VPN) está a criar um ambiente híbrido com atributos mais favoráveis aos criminosos, onde os utilizadores podem aplicar padrões de segurança e anonimato da web escura nas suas interacções na web superficial.

A Avaliação da Ameaça de Crime Organizado na Internet da Europol (*Internet Organized Crime Threat Assessment* – IOCTA) declara que a maior parte do CSAM ainda é partilhado em redes de partilha de filheiros em P2P.[34]. As plataformas de redes sociais e comunicação acessíveis publicamente continuam a ser os métodos mais comuns para conhecer e aliciar crianças online. Em 2018 o Messenger do Facebook foi responsável por quase 12 milhões das 18,4 milhões de denúncias mundiais de CSAM.[35]Estas denúncias podem vir a desaparecer se a encriptação de ponta-a-ponta for implementada por defeito, uma vez que as ferramentas actuais para detectar CSAM não funcionam em ambientes encriptados de ponta-a-ponta. Além disso, as redes de partilha de ficheiros em P2P proporcionam um manto para os criminosos poderem aceder e partilhar CSAM.[36]

O aumento da "encriptação por defeito" contribui para os crimes na web superficial, onde a crescente consciencialização do público para os riscos de segurança online e a vontade de proteger a privacidade das comunicações privadas contribuindo para a tendência de muitos serviços líderes de e-mail e envio de mensagens passarem a uma encriptação por defeito. Isto encoraja mais criminosos, incluindo os menos capazes tecnologicamente, a partilhar CSAM, dicas e técnicas em segurança e anonimamente. O WhatsApp, oferecendo encriptação de ponta-a-ponta aos seus utilizadores, foi o serviço de mensagens mais popular em 133 países e territórios em 2018.[37]

Com a tendência de mais e mais serviços convencionais virem a adoptar encriptação de ponta-a-ponta, ou a oferecer serviços efémeros (tais como a auto-eliminação de mensagens e imagens), os líderes governamentais estão a insistir junto dos seus homólogos na indústria para que assegurem que a privacidade e segurança online não seja ganha

às custas de nos deixar mais vulneráveis no mundo real. Continua o debate público sobre a protecção da privacidade dos utilizadores e a protecção de indivíduos, especialmente de crianças e adultos vulneráveis, contra danos criminosos.

O fórum da Child's Play na web escura

Um criminoso americano e um canadiano foram presos por manterem dois dos maiores sites de CSAM na web escura, chamados “Child's Play” e “Giftbox”, em 2017. No seu auge estes sites tinham mais de um milhão de perfis de utilizadores registados (alguns utilizadores podiam ter mais do que um perfil), onde as mensagens na categoria de abuso mais grave foram vistas mais de 770.000 vezes.

Na sequência de uma investigação conjunta entre as forças policiais dos EUA, Canadá, Austrália, e Europa, com o apoio da Equipa de Operações Conjuntas da NCA, foram presos dois criminosos em Virgínia, EUA, depois de uma viagem do criminoso canadiano para conhecer o seu homólogo americano. Após a detenção e interrogação, os criminosos forneceram os nomes de utilizador, palavras-passe, e chaves de encriptação às forças policiais.

Com a autorização dos parceiros nas forças policiais europeias, as palavras-chave e os servidores foram passados a uma força policial australiana. Continuaram a gerir a Child's Play sob autoridade legal na Austrália, com um agente policial a actuar como administrador do site. As provas recolhidas contribuíram para a identificação e resgate de 12 crianças só no Canadá, mais de 100 casos de vítimas foram reencaminhados mundialmente, e um país identificou cerca de 900 suspeitos.

Os dois criminosos receberam uma pena de prisão de 35 anos cada um pela administração de um empreendimento de exploração de crianças, e em 2017 foram ambos condenados a prisão perpétua pela violação de um menor.[38]

As aplicações móveis de mensagens mais populares no mundo

WhatsApp
A aplicação de mensagens mais usada no mundo, com encriptação de ponta-a-ponta por defeito.

Messenger do Facebook
A aplicação distinta de mensagens do Facebook permite aos seus utilizadores partilhar ficheiros, localização, e o envio de dinheiro em alguns mercados. Espera-se que venha a incluir conversas de ponta-a-ponta.

WeChat
A aplicação mais popular na China, com mais de mil milhões de utilizadores; permite a partilha de fotografias, chamadas de vídeo e de voz, partilha de localização, pagamentos digitais e jogos. Esta aplicação usa encriptação de transporte, onde a mensagem é encriptada entre o utilizador e os servidores da WeChat.

Viber
Mais de mil milhões de utilizadores; oferece mensagens encriptadas e *chats* auto-eliminados

Line
Muito popular na Ásia, com mais de 600 milhões de utilizadores. Chamadas para linhas fixas, e chamadas gratuitas linha-a-linha de vídeo ou voz. Permite *chats* encriptados.

Telegram
Milhões de utilizadores activos e *chats* altamente seguros encriptados.[39]

A encriptação de ponta-a-ponta cria risco para as crianças porque evita que as plataformas online e os seus moderadores consigam identificar, eliminar e denunciar conteúdos nocivos de partes críticas das suas próprias redes. Apesar disso, muitos fornecedores de serviços parecem estar a acelerar a implementação de encriptação de ponta-a-ponta e a aplicar tecnologias adicionais que também encriptam o nome da página de Internet que um criminoso esteja a solicitar.[40]A tecnologia de protocolos (conhecida como "sistema de nomes de domínio" (*domain name system* – DNS) sobre HTTPS, ou "DoH" (DNS over HTTPS)) implica levar o nome de um domínio que um utilizador tenha escrito no seu browser e o envio de uma busca a um servidor DNS para recolher o endereço numérico de IP do servidor de internet que aloja a página de Internet em questão. É também assim que o DNS funciona. Contudo, o DoH leva a busca de DNS a um servidor compatível com DoH (o "resolvedor") através de uma ligação de HTTPS encriptada, em vez de texto simples. Desta forma, o DoH esconde as buscas de DNS dentro do tráfego normal de HTTPS, não permitindo assim que observadores terceiros consigam monitorizar o tráfico e identificar as buscas de DNS que os utilizadores tenham feito e inferir que páginas de Internet estão prestes a aceder. Este factor pode ter um impacto nos mecanismos actuais para bloquear endereços de Internet que contenham CSAM e fazer com que os filtros de controlo parental ou da escola não sejam eficazes. O mundo da tecnologia continua ainda a debater as vantagens e desvantagens, mas o DoH já foi implementado em pelo menos um *browser* muito usado, havendo planos para incluir o DoH "por defeito" nos EUA, e os outros *browsers* estão a fazer planos semelhantes.

Enquanto as aplicações da web superficial oferecem acesso a CSAM a criminosos com poucas capacidades tecnológicas, os criminosos mais sofisticados e os que procuram mais recursos para tentar evitar serem detectados são mais atraídos pela web escura. Estes serviços podem apenas ser acedidos através de "redes sobrepostas", sendo necessário software especial para aceder a estas redes. Podem fazê-lo recorrendo a VPNs, redes de P2P, e ao método da Tor, conhecido por "roteador cebola", onde os dados de um utilizador são encriptados e depois transferidos por camadas diferentes para criar uma encriptação multi-camada – protegendo a identidade e a localização do utilizador.[41]O Departamento de Justiça dos EUA (*Department of Justice* – DoJ) indica que as páginas de Internet da web escura estão a crescer à razão de 40.000 por mês, continuando activas durante muitos anos.

As "consequências devastadoras" da encriptação para as crianças

No ano passado as forças policiais na UE receberam mais de 600.000 denúncias de casos de OCSE.

O resgate de uma menina de nove anos abusada pelo seu pai durante mais um ano, e de 11 crianças exploradas por uma rede de criminosos de abuso sexual de crianças, são apenas dois exemplos de casos com que as forças policiais da UE lidam diariamente.

A Comissária da UE dos Assuntos Internos lançou o aviso sobre as consequências devastadoras para as crianças na UE se as aplicações de mensagens forem encriptadas e as forças policiais deixarem de poder receber os relatórios que recebem actualmente.[42]

Tal como no aumento do uso da Internet no Sul Global, houve um aumento semelhante no uso destas técnicas. O site Projecto Tor declara que os utilizadores dos EUA, Rússia, Alemanha, França, Reino Unido, Ucrânia e Países Baixos constituem mais de metade (~55%) dos utilizadores da Tor. Contudo, durante os últimos dois anos, a proporção de utilizadores do Irão, Indonésia, e Índia aumentou em 14%.[43]É importante notar que estes dados representam o aumento na Tor, a qual pode ser usada tanto para actividades legítimas, como ilegítimas, incluindo activismo sobre os Direitos Humanos e liberdade de expressão.

Escondidos à vista

Os criminosos continuam a procurar novas formas de partilhar CSAM sem serem detectados pelas forças policiais, nomeadamente em "páginas de Internet disfarçadas" que usam técnicas de alojamento avançadas para permitir que as páginas de CSAM se escondam à vista de todos. A mesma página de Internet que revela imagens legais ao utilizador (ou investigador) casual quando abre o URL do site, revela CSAM a um utilizador que tenha visitado uma sequência de sites antes de chegar à página alvo. O alinhamento correcto de *cookies* serve como chave para abrir o conteúdo disfarçado quando o criminoso completa a sequência.[44]

O termo "sem soberania" refere-se à soberania de dados: a ideia de que os dados estão sujeitos às leis e estruturas governamentais da nação onde forem recolhidos. Os serviços sem soberania atravessam fronteiras nacionais e foram concebidos intencionalmente para operar fora de uma jurisdição claramente definida, permitindo assim aos criminosos a produção de material numa jurisdição e o seu alojamento noutra, para consumidores numa terceira localização, tornando quase impossível a tarefa de executar mandados ou notificações por governos nacionais e organização de forças policiais sem cooperação internacional sofisticada.

Aplicações sem soberania

O Departamento de Justiça dos EUA (*Department of Justice* – DoJ) tentou identificar e proteger um menor que está a ser coagido a auto-gerar imagens indecentes para um grupo de criminosos, usando uma aplicação popular de rede social e mensagens.

Esta aplicação foi "concebida sem soberania" e a empresa promove o facto de que nunca passou nenhuma informação a nenhum governo. O DoJ dos EUA tentou contactar a empresa através de canais diferentes, procurando apenas a informação do utilizador na esperança de identificar a vítima.

Todas as tentativas falharam, sendo a citação devolvida ao emissor.[45]

Um outro desafio para as forças policiais é a utilização de Redes de Distribuição de Conteúdos (*Content Delivery Networks* – CND), ou "serviços de passagem" que copiam as páginas de um sítio web para uma rede de servidores dispersos geograficamente por localizações diferentes. Quando um utilizador pede uma página que faz parte de uma CDN, a CDN redirecciona o pedido do servidor original da página para um servidor na CDN mais próximo do utilizador e entrega o conteúdo. O processo de saltos através das CND é quase invisível para o utilizador. A única forma de um utilizador saber se acedeu a uma CDN é se o URL recebido é diferente do URL pedido.

Novos tipos de crimes de tecnologia de ponta

O CSAM online está a ser partilhado através de variadíssimas formas que, há poucos anos, ou não existiam, ou eram de acesso muito restrito. A transmissão ao vivo pela Internet de abuso, "abuso por encomenda", e SGII são alguns exemplos, tal como a presença de material em sistemas de plataformas de distribuição. A chegada da encriptação, da realidade alternativa, virtual, e aumentada, e a descentralização da Internet estão já a ter um impacto na produção de CSAM e na forma como o material é distribuído e consumido.

2% das queixas recebidas na linha de apoio da República da Irlanda INHOPE em 2018 diziam respeito a "imagens virtuais de abuso sexual de crianças", [46] e investigadores na Alemanha encontraram 274 links de abuso sexual de crianças dentro da cadeia de blocos da Bitcoin.[47]

A tecnologia permite também cada vez mais aos criminosos a transmissão internacional em directo pela Internet de abuso por contacto "na sala", ocorrendo a maioria destes casos nas Filipinas.[48]Nas nações do Sul Global, com níveis mais altos de pobreza e um grande número de crianças vulneráveis, aumentam os riscos associados à combinação da adopção rápida de ligações de alta velocidade à Internet e a disponibilidade de dispositivos ligados à Web relativamente baratos.

Uma das grandes dificuldades com a transmissão em directo pela Internet é a dificuldade de detecção e policiamento do "acto ao vivo". Isto deve-se ao desafio de interceptar o conteúdo encriptado de canais de comunicações privados que atravessam fronteiras internacionais, e a indesejabilidade (na perspectiva da privacidade do público e liberdades civis) de autorizar intrusões sem direcção especifica. Resulta daí um aumento das chamadas tanto de fornecedores de serviço e governos para uma regulamentação melhor dos serviços que facilitam a transmissão em directo pela Internet de conteúdo ilícito.

A melhor oportunidade de identificar criminosos e proteger as vítimas é durante a fase em que o criminoso está a negociar o seu acesso a uma criança vulnerável (abordando e organizando a transacção com as famílias e indivíduos que facilitam este tipo de abuso); e quando as imagens ou gravações são capturadas e subsequentemente partilhadas através de portais online e fóruns de Internet.

Abuso transmitido ao vivo pela Internet no mundo

Uma investigação conjunta de forças policiais da Austrália, Alemanha, Filipinas, e dos EUA resultou na apreensão de criminosos por envolvimento na produção e distribuição de CSAM. Um dos criminosos, australiano, foi apanhado a dirigir transmissões ao vivo pela Internet de crianças a serem abusadas por uma mulher. A mãe das crianças abusava sexualmente das suas três filhas em ciber-espectáculos há vários anos. A mulher recebia e recolhia transferências de dinheiro dos espectadores numa agência de câmbio usando duas identidades diferentes.

Depois de terem sido resgatadas pelas forças policiais, uma das crianças identificou uma fotografia de um outro criminoso australiano, levando a um subsequente reencaminhamento para as autoridades australianas e à detenção de criminosos na Austrália e na Alemanha. Cada nova investigação gerava novas pistas, e gerou-se um elo de reencaminhamentos da Austrália às Filipinas, das Filipinas de novo à Austrália, e das Filipinas à Alemanha, continuando a revelar novas pistas. Demonstra-se, assim, o valor dos ciclos "investigação-reencaminhamento-investigação" e os benefícios de partilha de informações com agências policiais internacionais.[49]

Sistemas de pagamentos móveis contornam a necessidade de registo e verificação de identidade

As tecnologias de pagamento de acesso a CSAM continuam a evoluir. Ao passo que as intervenções de sucesso de coligações financeiras levaram a uma redução da quantidade de imagens pagas por cartão de débito ou de crédito, os serviços de pagamento online, de transferência de dinheiro, e centros locais de pagamento são agora mais usados.

Um método popular de pagamento é o Sistema Informal de Transferência de Valores (*Informal Value Transfer System* – IVTS), que usa telemóveis sem a necessidade de um cartão de crédito ou sequer uma conta bancária. O dinheiro pode ser cobrado usando apenas um número de telemóvel e um número de referência, não sendo necessário um registo e identificação formais.[50]Os criminosos adoptam sempre novas tecnologias logo muito cedo, tais como as criptomoedas, para aceder e partilhar CSAM dissimuladamente. Em Julho de 2018 as forças policiais búlgaras prenderam oito suspeitos envolvidos na disseminação de CSAM. Os criminosos usaram Bitcoin para pagar o alojamento de um sítio web criado especificamente para depositar imagens e vídeos de abuso sexual de crianças.[51]

Recentemente as forças policiais têm notado um aumento de mercados online alojando e comercializando CSAM na web escura. Para ganhar acesso, os utilizadores têm de pagar uma quantia de dinheiro ou fornecer CSAM de "primeira geração".[52]

A tecnologia é simultaneamente uma facilitadora nociva, e parte integral da solução

A tecnologia não proporciona apenas a crescente prevalência de CSAM, mas também capacita as forças policiais, a indústria da tecnologia, e organizações do sector terciário na identificação, denúncia e prevenção de CSAM, e a identificar e localizar as vítimas e os criminosos.

As técnicas de investigação inovativas, tais como a inteligência artificial (IA), rastreio, prevenção de sítios web e bloqueio de imagens, podem ser todas usadas para proteger crianças online. Por exemplo, a campanha "Seguir um Objecto" (*Trace an Object*) da EUROPOL, lançada em Maio de 2017, usou a participação colectiva do conhecimento social para identificar objectos retirados do plano de fundo de uma imagem com material sexualmente explícito envolvendo menores.[53]Rastrear uma vítima apenas pela sua imagem é um desafio. Contudo, o CSAM contém frequentemente objectos identificáveis no plano de fundo, desde objectos de consumo, a mobília e características arquitectónicas distintas, o que pode ser essencial para estreitar a localização do abuso e proteger a vítima.

A visão dos EUA, Canadá, Reino Unido, Austrália, e Nova Zelândia

Este ano, numa reunião de Ministros da Austrália, Canadá, Nova Zelândia, Reino Unido e Estados Unidos da América, houve consenso na firmeza de que as empresas de tecnologia não devem desenvolver sistemas e serviços em formatos que possam capacitar criminosos ou pôr indivíduos vulneráveis em risco. Em vez disso, as empresas de tecnologia devem dar prioridade à protecção dos seus utilizadores e do público em geral quando concebem serviços.

Os participantes concordaram que o combate da epidemia de exploração sexual de crianças online necessita de uma ampliação imediata da resposta mundial para assegurar que todas as crianças no mundo são protegidas, e que não haja nenhum espaço seguro online onde os criminosos possam operar.[54]

05 Mudanças de comportamento dos autores de crimes

A intensificação da sofisticação técnica contribui para o crescimento do número de crimes, aumento de abuso, e dificultação das investigações

Por todo o mundo há ainda áreas deficientes na compreensão das causas e origens do comportamento sexual abusivo, surgindo cada vez mais investigações no Norte Global. Compreendemos muito menos o percurso de crime nos indivíduos com um interesse sexual em crianças, do que o dano online causado pela distribuição de conteúdo online relacionado com terrorismo e extremismo.

Após vários anos de estudo os psicólogos conseguem agora determinar como indivíduos vulneráveis são radicalizados para ideologias extremistas, podendo implementar medidas que ajudam a prevenir o seu agravamento e encorajar os radicalizados a desistir e se separar da actividade. No entanto, não é claro se é possível adaptar técnicas semelhantes para dissuadir indivíduos do primeiro crime de abuso sexual de crianças, de ver CSAM, e de incitar ou efectuar abuso por contacto “ao vivo”.

Um estudo de crimes sexuais adultos gerais, preparado pelo Gabinete dos EUA de Crimes Sexuais, Condenação, Monitorização, Apreensão, Registo e Rastreio (*Sex Offender Sentencing, Monitoring, Apprehending, Registering and Tracking* – SMART) revelou que o problema de crimes sexuais é complexo demais para se poder atribuir a uma só teoria.[55]As teorias de factores múltiplos ajudam a compreender melhor as causas dos delitos sexuais.

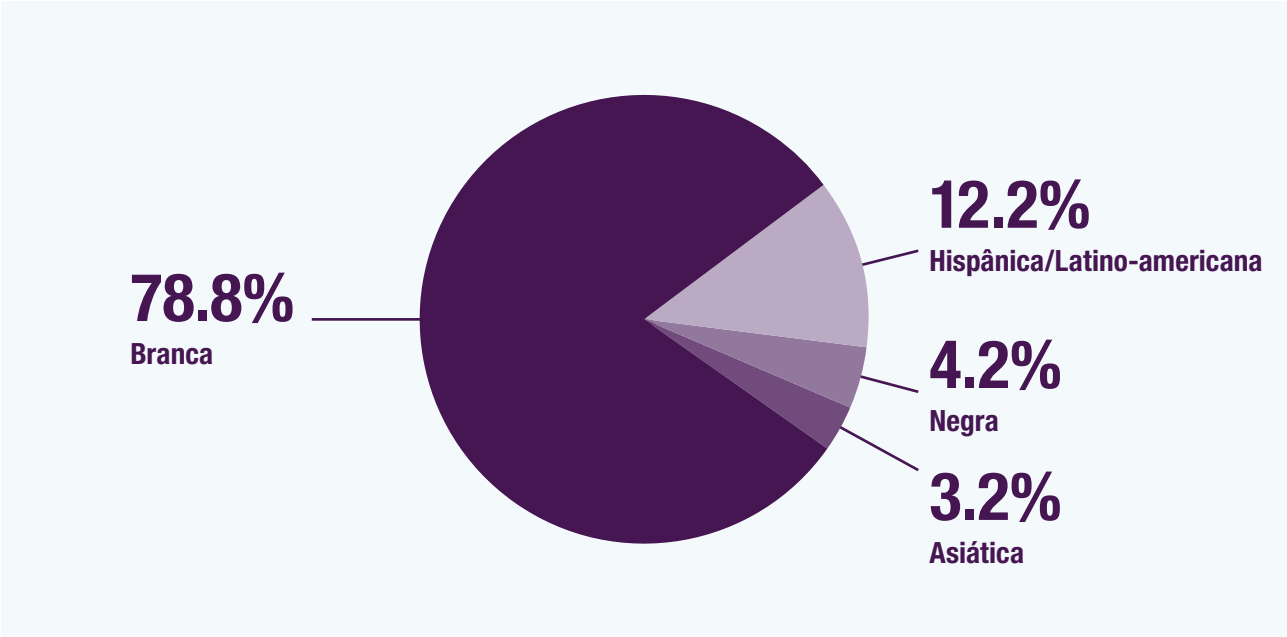
O que sabemos:

- nem todos os indivíduos com um interesse sexual em crianças cometem o crime (notando que a execução de abuso por contacto ao vivo, a coação da produção de actividade sexual online, e o ver imagens online constitui um delito).
- nem todos os criminosos são pedófilos (uma orientação sexual em adultos e tardo-adolescentes que orientam os seus sentimentos e desejos sexuais ou eróticos para crianças pré-pubescentes). os efebófilos revelam uma atracção sexual adulta principalmente dirigida a pubescentes. ambas as categorias devem ser distinguidas nos indivíduos com condições clínicas de pedofilia e efebofilia que são violentos contra as crianças.
- as condições adversas ou negativas no desenvolvimento inicial – especialmente más relações com prestadores de cuidados – podem contribuir para este comportamento.

Apesar de o número de casos de OCSE estar a aumentar, esse aumento deve-se, em parte, aos métodos cada vez mais sofisticados que os países e prestadores de serviços de Internet (ISPs) têm agora à sua disposição para identificar e eliminar CSAM, e também encontrar os criminosos. Tudo isto está a contribuir para que compreendamos melhor o perfil do criminoso.

A GTA18 concluiu que os criminosos podem vir de qualquer idade, raça, sexo, profissão, estatuto socio-económico ou área geográfica. A análise subsequente de dados da INTERPOL sobre Exploração Internacional Sexual de Crianças (*International Child Sexual Exploitation* – ICSE), nas suas bases de dados de imagens e vídeo, indica que 92,7% dos criminosos eram homens, as mulheres criminosas surgiam mais frequentemente juntamente com um homem criminoso, a maior parte das vítimas eram da mesma etnia da dos criminosos, e a maioria dos criminosos (78,8%) eram brancos (notando-se, contudo, que em mais de 75% dos casos era impossível determinar a etnia do criminoso, e que as proporções reduzidas de alguns grupos étnicos podem ser o resultado da ausência de alguns países associados à base de dados de ICSE).[56]

Figura 5: Etnia de criminosos visíveis[57]



A investigação conjunta da INTERPOL e da ECPAT sobre vítimas não identificadas de CSAM recomendou a criação de estruturas abrangentes para a categorização de características de vítimas e de criminosos, tais como etnia, em todas as regiões e países.

Estamos também a verificar o surgimento de uma geração mais nova de criminosos. Cresceram com a tecnologia e, por isso, conhecem bem e estão mais à vontade com as TI. Daí que há um grupo de criminosos mais susceptíveis de identificar e explorar técnicas e serviços avançados de segurança para evitar a deteção.

Em Queensland, na Austrália, um estudo publicado em 2018 confirmou que quase metade dos 3.035 criminosos processados pelo sistema penal por casos de CSAM eram, eles próprios, menores com menos de 17 anos de idade, onde o número de criminosos advertidos por posse de SGII aumentou mais de dez vezes entre 2006 e 2016.[58]

Além disso, esta geração é menos susceptível de denunciar imagens sexuais de crianças: a campanha recente da IWF "#SoSockingSimple" revelou a falta de consciencialização e compreensão entre os jovens adultos masculinos de que ver CSAM é ilegal e deve ser denunciado.[59]

A Avaliação Estratégica Nacional de 2019 da Agência Nacional de Crime do Reino Unido (National Crime Agency – NCA) identificou a razão principal de OCSE como gratificação sexual. Outros procuram ganhos financeiros com a venda de CSAM online (especialmente de abuso transmitido ao vivo), ou a monetização de tráfego de Internet relacionado com CSEA através de publicidade de "pagamento por clique".[60]A transmissão de abuso ao vivo na Internet para fins comerciais é uma ameaça crescente: por um custo modesto de €10-€20, os criminosos podem organizar o abuso, em tempo real, de uma criança à escolha.[61]E, para alguns, CSAM é usado como moeda de troca dentro das redes de abuso de crianças. Os criminosos usam o material para ganhar notoriedade ou para negociar fotografias e vídeos novos, que ninguém tenha ainda visto.

A maior parte dos criminosos ainda pode ser classificado como indivíduos muito reservados e privados. Contudo, a criação dos presumidos "portos seguros" digitais está a contribuir para uma tendência crescente onde os criminosos se reúnem em fóruns da web escura e plataformas dos prestadores de serviços de Internet com serviços encriptados de envio de mensagens e transmissão ao vivo. Aqui, os criminosos não estão somente a ver imagens. Dirigem-se activamente a crianças por todo o mundo através de plataformas comerciais para manipular e extorquir imagens explícitas ou para conseguir acesso cara-a-cara.

Além disso, a fácil disponibilidade de CSAM na Web superficial facilita a possibilidade de cometer o crime. Estas comunidades normalizam o comportamento dos criminosos, encorajam e validam, e capacitam os criminosos a partilhar e ganhar experiência, desse modo diminuindo a possibilidade de esses indivíduos chegarem a pedir ajuda e aumentando as possibilidades de agravar o seu comportamento criminoso. A falta de factores de dissuasão e serviços de apoio também podem ser um factor contributivo, uma vez que os indivíduos com um interesse sexual em crianças podem não saber como pedir ajuda, mesmo que o quisessem fazer.

Potenciais percursos de agravamento

Normalmente a lei distingue entre os que recolhem CSAM para colecções pessoais e os que adquirem e partilham CSAM activamente, e também entre os que praticam contacto pessoalmente e ao vivo e aqueles cujos actos de abuso de menores é praticado exclusivamente online.

Estas distinções são importantes, porque indicam um possível percurso de agravamento a partir de, por exemplo, os que procuram e vêm imagens pré-existentes e os que manipulam ou coagem crianças para um comportamento sexualmente explícito nas suas próprias câmaras web (incluindo abuso onde a vítima se toca a si própria ou abuso entre duas vítimas), e entre os que pagam para dirigir e observar o abuso perpetuado por um criminoso "na sala" e os que praticam o abuso eles próprios por contacto.

Contudo, o agravamento não é inevitável, por isso há muitas oportunidades de intervenção para prevenir ou dissuadir os indivíduos que a EUROPOL descreve como "simples observadores", permitindo que as organizações das forças policiais se concentrem nos criminosos mais graves e continuados. De acordo com a UNICEF, é provável que a maior parte dos criminosos online sem antecedentes de crimes por contacto não passe a crimes por contacto no prazo de um a cinco anos do seu primeiro crime.[62]Mas também se compreende cada vez mais que o abuso online conduz a um risco maior de desvio sexual, uma vez que o comportamento criminoso está menos constrangido pelo medo de detecção ou identificação.[63]

Mudar o percurso dos criminosos

Vários casos lidados pela NCA revelam como a tecnologia está a mudar a forma como alguns criminosos praticam o abuso, a depravicidade do abuso, e o percurso do próprio criminoso.

Num caso, um criminoso filiou-se numa discussão privada online de um grupo de indivíduos com interesse sexual em menores. Os novos membros do grupo tinham de publicar imagens novas e, consequentemente, o criminoso violou uma menina de seis meses e molestou um menino de dois anos, publicando depois os vídeos numa aplicação encriptada, partilhando-os através de um site popular de partilha de ficheiros.[64]

Num outro caso um criminoso estava a enviar dinheiro a facilitadores conhecidos especializados em transmissão ao vivo pela Internet de abuso sexual de crianças nas Filipinas, e foi preso quando regressou ao Reino Unido. A análise forense indicou que o criminoso tinha enviado um mínimo de 15 transferências de dinheiro aos facilitadores entre Agosto de 2017 e Junho de 2018, tendo sido encontradas imagens de abuso de menores no seu telemóvel.[65]

Um outro criminoso foi preso em Fevereiro de 2018 por 25 anos, depois de se declarar culpado de 137 crimes relacionados com 300 vítimas de "material duro de dor" na web escura. O criminoso conseguiu acesso a crianças online coagindo-as e chantageando-as através de fóruns abertos e sítios de comércio electrónico, antes de transferir a conversa para plataformas seguras e encriptadas para praticar sextorção e chantagem. O criminoso forçou as vítimas a praticar actividades cada vez mais depravadas ameaçando-as com a distribuição de imagens e dados pessoais na web escura. [66,67]

Casos como estes demonstram o agravamento e incitação à prática do crime através de redes de pares tanto na web superficial como na web escura, onde as conversas entre indivíduos com mentalidades semelhantes leva os criminosos a partilhar métodos de praticar os crimes e evadir detecção.

No seu conjunto, estes casos de estudo são indicativos de uma mudança do percurso dos criminosos e da clara relação entre o abuso por contacto directo e indirecto.

Alguns criminosos que foram presos por ver e possuir imagens indecentes de crianças alegam que não cometeram nenhum crime porque não houve abuso por contacto, e que não estavam envolvidos em nenhuma forma de coação, especialmente quando foram as próprias crianças que publicaram as imagens e os vídeos. Em 150 dos 195 países abrangidos pelo Projecto de Direito do Centro Nacional de Crianças Desaparecidas e Exploradas (*National Center for Missing and Exploited Children* – NCMEC), a legislação doméstica está agora de acordo com o Critério 4, o qual criminaliza a posse consciente de CSAM independentemente da intenção de distribuição.[68]

Numa perspectiva de protecção, a distinção entre abuso "de contacto" e "sem contacto" é falaciosa. Quando um criminoso não está fisicamente presente na sala, mas orienta a prática remotamente, as vítimas de "abuso de contacto onde a vítima se toca a si própria" revelam um sentido de culpa e vergonha mais agudo, dificultando a recuperação.[69]

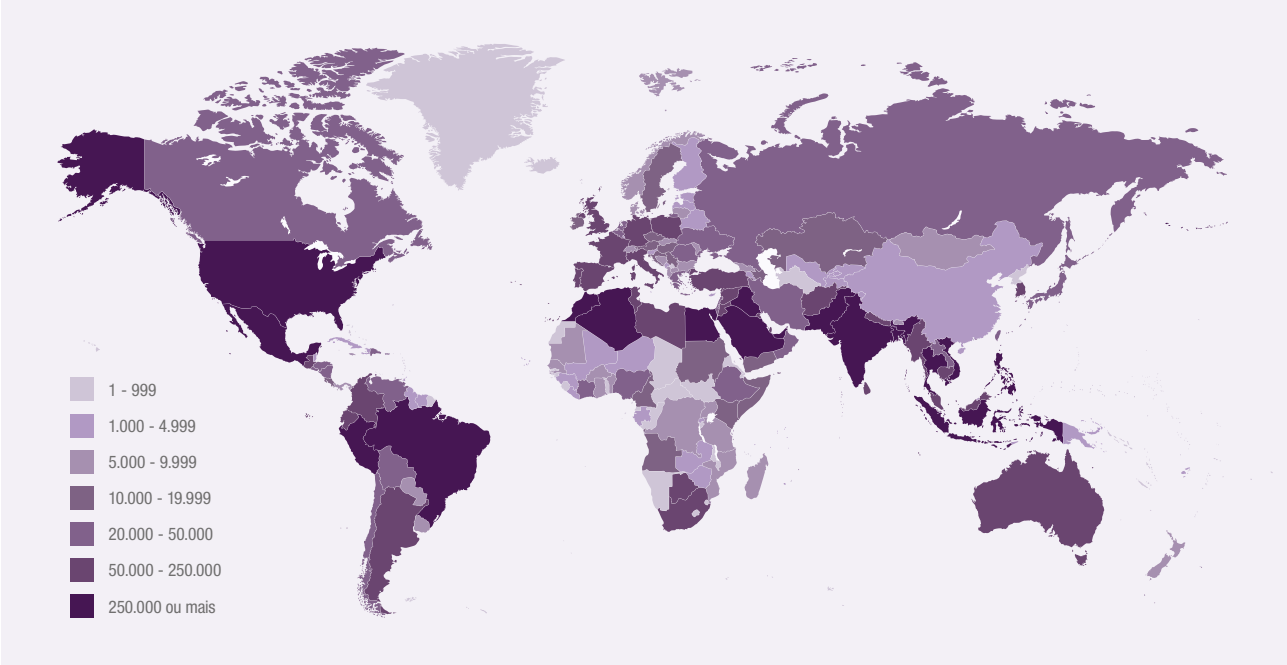
A demografia dos criminosos reflecte a sua comunidade

Um estudo do Centro Especializado de Abuso Sexual de Crianças, do Reino Unido (*Centre of Expertise on Child Sexual Abuse* – CSA Centre) revelou que, no Norte Global, a contribuição de emprego e económica dos criminosos era consistente com as proporções nas suas comunidades.[70]Por exemplo, a investigação da Associação Britânica de Assistentes Sociais (*British Association of Social Workers* – BASW) descobriu que o protótipo de criminoso online no Reino Unido era um homem branco, solteiro, na casa dos vinte ou trinta anos, bem educado, empregado, sem um historial de doença mental grave ou adversidade infantil significativa.[71]Este achado está em conformidade com os dados de organizações das forças policiais e não-governamentais, os quais revelam que os criminosos de CSEA online são desproporcionalmente homens.

Estas conclusões podem não ser verdadeiramente representativas. Uma grande parte dos crimes não são denunciados e os crimes por mulheres não é suficientemente detectado ou denunciado.[72]É pouco provável que o perfil actual geral do criminoso reflicta a demografia dessas nações mais afluentes, as quais gozaram do maior crescimento de penetração tecnológica, posse de dispositivos, e acesso à Internet.

Tal como estabelecemos no Capítulo 4, não é possível correlacionar com precisão a demografia dos que produzem, alojam, e consomem CSAM, uma vez que todas estas actividades podem ocorrer em jurisdições diferentes.

Figura 6: Relatório NCMEC de 2018



O mapa térmico dos relatórios do NCMEC de 2018, resumido na página anterior, mostra a origem da maior concentração de denúncias de suspeita de CSAM, salientando a escala global do problema.[73]

Estatísticas de URL da IWF

87% dos URLs de abuso sexual de crianças identificados no mundo pela IWF estão alojados só em cinco países: Países Baixos, Estados Unidos da América, Canadá, França, e na Federação Russa.[74]

Criminosos de baixa tecnologia e peritos em tecnologia

Embora não haja uma correlação directa entre literacia técnica e comportamento criminoso, o aumento da sofisticação técnica sugere a diminuição da probabilidade de detecção e apreensão, e o aumento da complexidade da tarefa do investigador.

Enquanto que o GTA18 salientava a emergência de comunidades de criminosos a usar plataformas muito seguras, encriptadas, e anónimas, as quais necessitavam de um nível de peritagem técnica muito elevado, há agora uma nova vaga de criminosos capacitados por serviços gerais para consumidores com um baixo custo de entrada.

As maneiras diferentes usadas pelos criminosos para conseguir acesso a crianças

As recentes estatísticas publicadas pelos tribunais da China indicam que as vítimas e os criminosos em casos de abuso sexual de crianças se contactaram pela Internet em cerca de 30% de todos os casos denunciados. Contudo, os oficiais do tribunal notam que "o abuso sexual de crianças é um crime altamente sub-denunciado, uma vez que acontece frequentemente em ambientes privados", e muitos não chegam a processos legais devido a "razões objectivas e subjectivas", incluindo o medo das vítimas e os desafios na obtenção de provas.

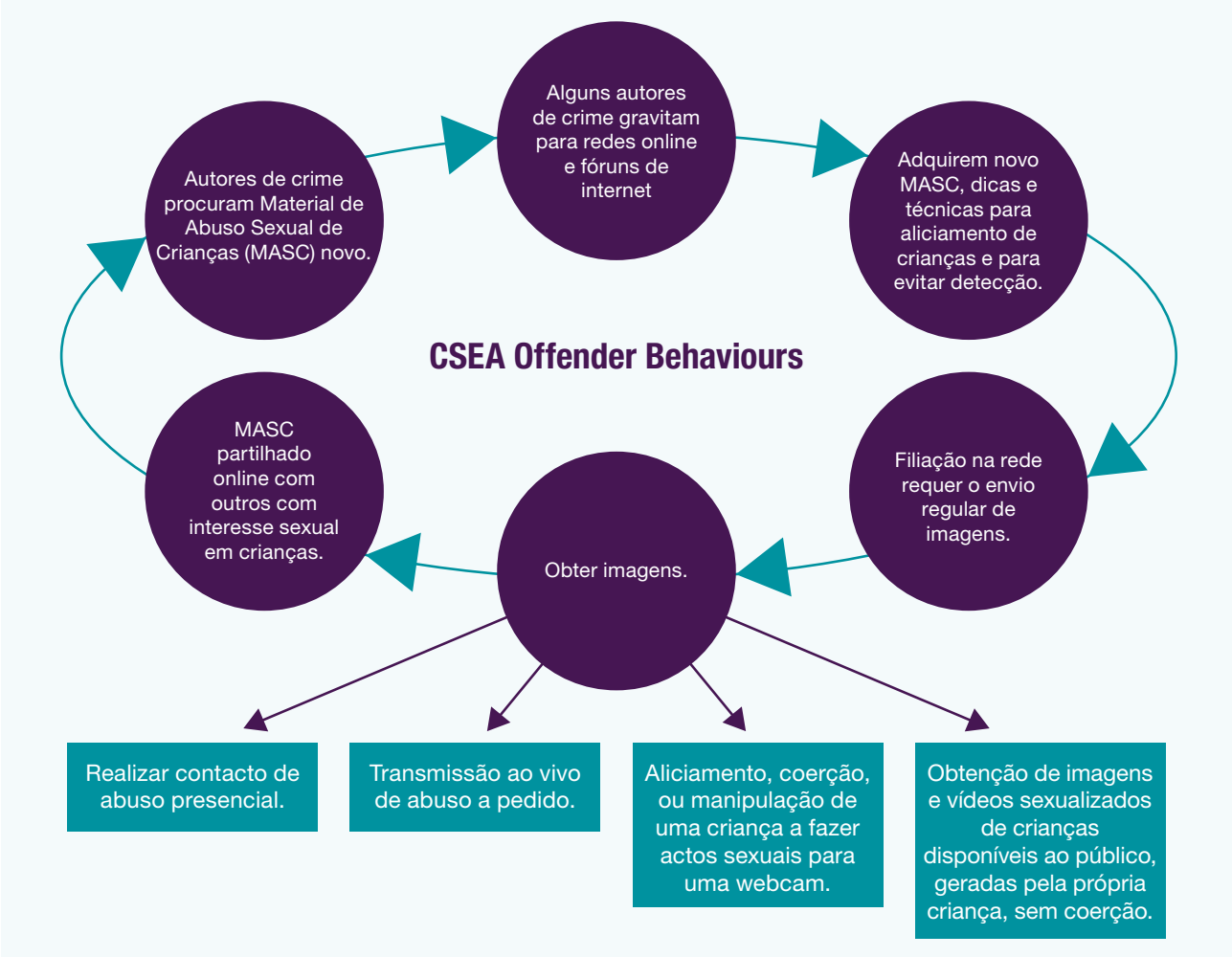
Num dos casos, um criminoso foi condenado a 11 anos de prisão por coagir as suas vítimas a enviar imagens sexualmente explícitas dizendo-lhes que era um executivo de televisão em busca de talento. O criminoso passou depois a usar estas imagens para chantagear as vítimas a enviar mais fotografias e vídeos. Num outro caso um homem de 32 anos de idade usou uma aplicação de namoro para se envolver com crianças, antes de abusar, num quarto de hotel, uma vítima que tinha conhecido pela aplicação.[75,76]

Outro caso revelou que um criminoso numa zona rural da China conseguiu acesso a boletins Tor. Quando o criminoso notou que a ligação lenta à Internet estava a limitar a sua capacidade de aceder ao Tor, mudou para sítios de partilha P2P, usando muitas vezes uma VPN para esconder o seu endereço IP.[77]

Estes casos de estudo revelam que os criminosos podem, e usam, uma gama ampla de tecnologia para aceder e explorar crianças, e este fenómeno é universal e não é exclusivo ao Norte Global.

Paralelamente, o crescente uso de redes sociais permitiu um acesso sem precedentes a crianças. Este crescimento levou a um aumento significativo de aliciamento online, chantagem e extorsão. Os criminosos podem concentrar-se simultaneamente em várias crianças, chantageando-as e extorquindo-as rapidamente. Consequentemente, o CSEA está agora associado ao aliciamento de crianças através das redes sociais. Contudo, as crianças continuam vulneráveis a abuso de contacto pessoal por membros das suas próprias famílias e por indivíduos em posições de confiança, e, em alguns países, este abuso está frequentemente associado ao tráfico de ciber-sexo.[78,79] Aliás, 67% de imagens de CSAM online aparentam ter sido tiradas num ambiente doméstico.

Figura 7: Comportamentos de Criminosos de CSEA



Muitos dos factores acima indicados conduzem a um ciclo vicioso de comportamentos de criminosos. A paisagem que nos surge é que os indivíduos com um interesse sexual em crianças procuram novas imagens indecentes e vídeos de crianças online, e que podem até procurar contacto pessoal com crianças. Uma melhoria na segurança e no anonimato significa que esses indivíduos são atraídos cada vez mais para redes e fóruns online, onde adquirem não só imagens, mas dicas e técnicas para aliciar crianças e evadir detecção. A criação de medidas de prevenção necessita de mais investigação para compreender as causas do comportamento sexual abusivo.

06 A visibilidade online das vítimas

Níveis mais elevados de acesso online e a evolução das normas culturais têm baixado a média de idades das vítimas e aumentado a sua vulnerabilidade

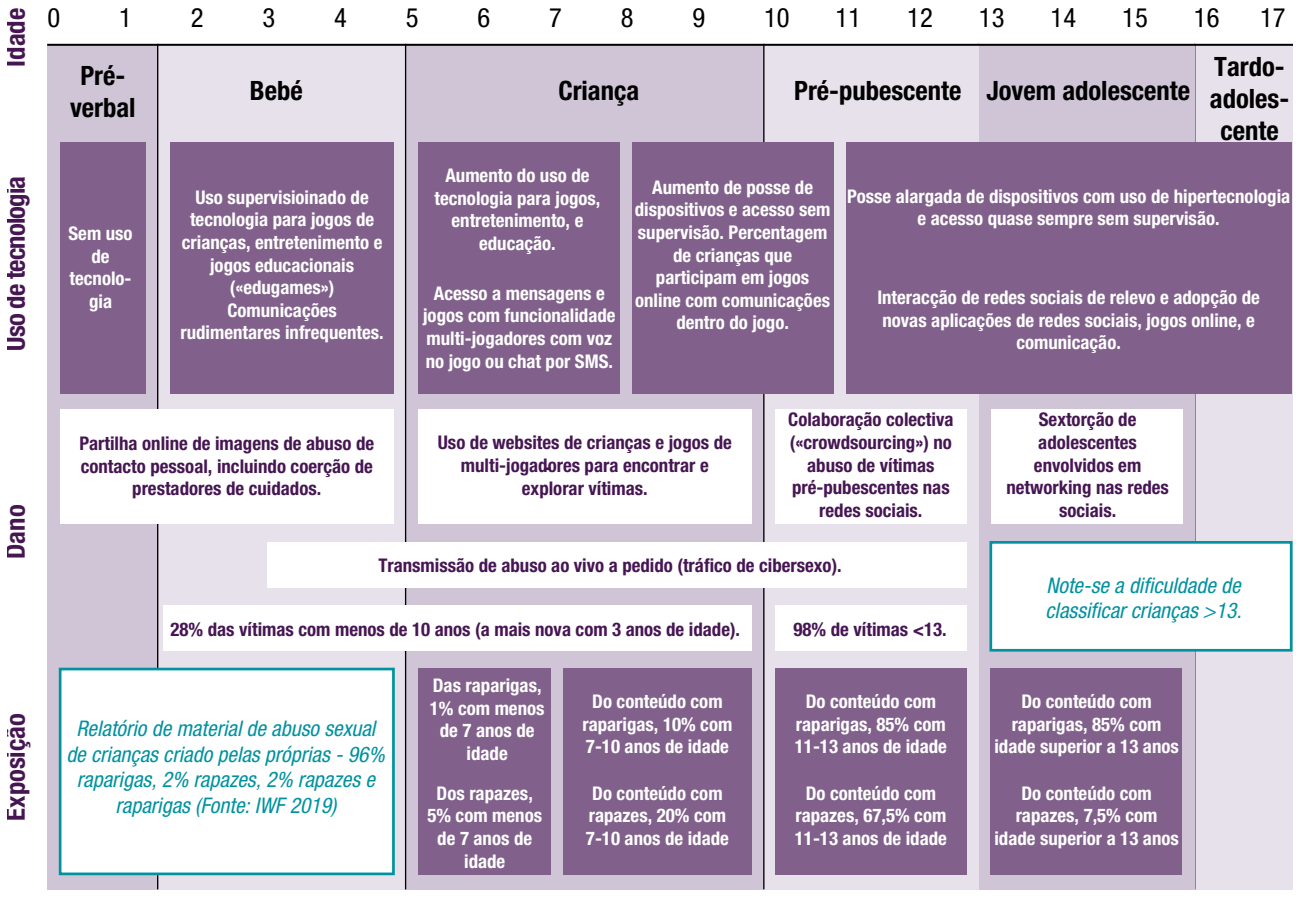
Categorizámos as vítimas do seguinte modo, de acordo com a sua idade e respetiva adoção de tecnologias. Novos dados, resultantes de pesquisas realizadas junto dos pais e de fóruns online relativos ao uso de redes sociais populares e serviços de jogos multijogador por parte das crianças, sugerem que a idade média dos utilizadores de cada tipo de tecnologia é, aproximadamente, dois anos mais baixa do que a primeira indicada no GTA18.

Quando categorizamos os mesmos grupos etários relativamente ao tipo de danos a que são expostos, bem como a percentagem de crianças em cada faixa etária que são expostas aos vários danos, há uma clara correlação com os tipos de tecnologia utilizados por cada grupo etário.

De acordo com a UNICEF, um em cada três utilizadores da Internet a nível mundial é uma criança.[80] Isto é o equivalente a 122 milhões de crianças a aceder à Internet só em 2018. Isto representa um desafio significativo para a supervisão e protecção por parte dos adultos.

As crianças estão a adquirir, e/ou a ter acesso a, dispositivos inteligentes com acesso à Internet em idades cada vez mais jovens e estão a utilizá-los para interagir com estranhos sem supervisão através das redes sociais de jogos multijogador online.[81] Isto expõe as crianças e pessoas vulneráveis a uma vasta gama de riscos (o Governo do Reino Unido identificou 29 categorias de danos online) dos quais a OCSE,

Figura 8: Categorização de vítimas de OCSE



o terrorismo online e o conteúdo extremista representam a maior escala e gravidade.[82]

Este problema é especialmente preponderante em sociedades prósperas. Muitos dos cuidadores e professores que têm um papel fundamental na definição dos termos do acesso online das crianças nunca vivenciaram estes riscos e danos nas suas próprias infâncias. Assim sendo, a consciencialização dos perigos que regem as normas das interacções físicas no mundo exterior ainda não se desenvolveram no mundo online.

Embora a idade mínima recomendada para criar uma conta nas redes sociais seja 13 anos, ou mais em algumas jurisdições (sendo que para o Facebook, Twitter, Instagram, Snapchat e outras empresas de redes sociais Americanas este seja um limiar mínimo previsto por lei) há indícios de acesso online generalizado e de posse de dispositivos por parte de crianças entre os 5 e 13 anos, bem como claras indicações de que as crianças estão a ser expostas ao mundo da Internet a uma idade mais jovem.

O impacto do acesso às redes sociais e a serviços de jogos sem supervisão é visível no perfil etário dos sujeitos de SGII, bem como nos resultados das pesquisas online realizadas junto de pais e utilizadores. O popular jogo online multijogador para crianças Fortnite® tem uma classificação etária do Sistema Pan-Europeu de Classificação Etária (*Pan European Game Information* - PEGI) de 12 anos mas, numa pesquisa online realizada em 2018 pelo Survey Monkey e a Common Sense Media, 26% dos pais indicaram 8-11 anos como a idade a que as crianças deveriam ser autorizadas a jogar.

42% das crianças na Austrália já utilizam dispositivos com acesso à Internet aos dois anos de idade e 81% aos quatro anos de idade

51% das crianças entre os 6 e 13 anos de idade na Alemanha têm um telemóvel ou telemóvel inteligente[83]

80% das crianças com menos de 14 anos de idade em Singapura já acederam à Internet[84]

90% das crianças entre os 11 e 16 anos de idade no Reino Unido dizem que têm uma conta nas redes sociais e 44% das crianças entre os 5 e 15 anos de idade tem um telemóvel inteligente[85]

Uso emergente das plataformas de jogos

Uma das técnicas usadas pelos criminosos consiste em oferecer a uma criança uma peça de equipamento ou algum dinheiro do jogo que a criança precise ou queira para um jogo específico. Um criminoso disse que viu uma jovem rapariga a fazer uma transmissão em directo no YouTube. Ele perguntou-lhe se ela gostava de um certo jogo e se queria algum dinheiro do jogo. Quando ela respondeu que sim, o criminoso perguntou-lhe qual era a sua identificação no jogo e começou a falar com ela na plataforma, acabando por receber imagens indecentes autogeradas em troca pelo dinheiro no jogo.[86]

Factores socioeconómicos

A vulnerabilidade online das crianças é intensificada por vários factores socioeconómicos e culturais. As crianças estão a adquirir, e/ou a ter acesso a, dispositivos inteligentes com acesso à Internet em idades cada vez mais jovens e estão a utilizá-los para interagir com estranhos sem supervisão através das redes sociais de jogos multijogador online. Isto expõe as crianças e pessoas vulneráveis a uma vasta gama de riscos dos quais a OCSE, terrorismo online e o conteúdo extremista representam os aspectos mais graves e de maior amplitude. Este problema é especialmente preponderante em sociedades prósperas. Muitos dos cuidadores e professores que têm um papel fundamental na definição dos termos do acesso online das crianças nunca vivenciaram estes riscos e danos nas suas próprias infâncias. Assim sendo, a consciencialização dos perigos que regem as normas das interacções físicas no mundo exterior ainda não se desenvolveram no mundo online.

Paralelamente, muitas pessoas no Sul Global estão a receber a gama completa de serviços instantaneamente, uma vez que a infra-estrutura de dados móveis e dispositivos de baixo custo permitem o acesso não regulado, sem o investimento correspondente na actualização da educação, legislação, serviços sociais e serviços de aplicação da lei. Isto é agravado por normas sociais diferentes relativas à sexualidade infantil e há desafios específicos relacionados com investigações e o apoio de vítimas do sexo masculino, especialmente em sociedades que pensam que os rapazes são resilientes e mais capazes de se protegerem a si próprios.[87]

De acordo com a Autoridade de Comunicações do Quénia, 88% dos 44 milhões de habitantes do país utilizam dispositivos móveis, embora 42% da população do Quénia viva abaixo da linha da pobreza e os níveis de desigualdade sejam dos mais elevados de África.[88] Em tais circunstâncias, as crianças nos grupos com rendimentos mais baixos correm riscos maiores de serem vendidas, abusadas ou traficadas online para trazer rendimentos às famílias.[89]

De modo semelhante, no Camboja, zonas económicas e de livre comércio especiais foram identificadas como especialmente problemáticas para a exploração sexual e tráfico de crianças, uma vez que as oportunidades económicas tornaram estes destinos populares entre as crianças e famílias de regiões mais pobres.[90]

Canadá
O projecto Canadiano Arachnid examinou 2 mil milhões de páginas Web a nível global à procura de material com abuso sexual de crianças desde 2016, emitindo mais de 4,6 milhões notificações de retirada a fornecedores de serviços Internet. 85% destas páginas dizem respeito a vítimas que, tanto quanto se sabe, não foram identificadas pelas autoridades de aplicação da lei[91]

Camarões, Gâmbia, Quénia, Togo e Uganda
54% das crianças viram alguém da sua idade em CSAM online e cerca de 10% das crianças foram contactadas por contactos online para partilharem imagens de natureza sexual[92]

México
12.300 contas da Internet estavam a distribuir CSAM no México em 2017[93]

Reino Unido
21% das raparigas inquiridas entre os 11 e 18 anos de idade receberam pedidos para enviarem imagens ou mensagens de natureza sexual.[94]

As comunidades deslocadas têm um nível de risco mais elevado

Há um conjunto de evidências cada vez maior que sugere que as crianças em comunidades deslocadas, incluindo refugiados e migrantes económicos, enfrentam um risco mais elevado de OCSE devido a uma jurisdição mais débil e à adopção de tecnologias em comunidades em que as capacidades de protecção de crianças são limitadas.

No Médio Oriente, o Comissário das Nações Unidas para os Refugiados descreveu casos de jovens refugiados Sírios no Líbano e na Jordânia chantageados por rapazes mais velhos para terem actividade sexual, os quais usam telemóveis secretamente para gravar imagens indecentes que ameaçam colocar na Internet.[95]

Na China, a instabilidade política de Estados vizinhos resultou em altos níveis de pessoas deslocadas, com comunidades de crianças especialmente vulneráveis. Serviços de mensagens e plataformas de redes sociais populares estão a ser utilizados para facilitar o tráfico sexual de mulheres e crianças de regiões rurais.[96]

A ameaça de deportação, p. ex. para migrantes da Coreia do Norte, pode fazer com que as vítimas tenham relutância em denunciar o abuso. Investigações da Korea Future Initiative salientam que crianças com apenas nove anos de idade aparecem em transmissões online de sexo em directo.[97] Esta vulnerabilidade está a ser especialmente explorada por sociedades da Ásia Oriental mais prósperas, incluindo a Coreia do Sul, onde o relatório de uma ONG indicou que 95% da exploração comercial de crianças é organizada através da Internet.[98]

Factores culturais

Os factores sociais também podem influenciar a vulnerabilidade a CSEA online: as crianças das comunidades lésbicas, gays, bissexuais e transgéneras (LGBT+) têm uma maior probabilidade de explorar a sua sexualidade online, o que pode aumentar a sua vulnerabilidade a chantagem e exploração e diminuir a probabilidade de denunciarem abuso.

Um estudo de CSAM online identificou que 80% das vítimas eram mulheres, 87% eram caucasianas e 83% dos criminosos adultos visíveis eram homens.[99] Com o a diminuição da separação tecnológica e com o aumento do acesso à Internet no Sul Global, antecipamos que estas estatísticas virão a tornar-se mais representativas de uma sociedade global e de factores culturais, divisão urbana/rural, acesso aos serviços de apoio e diferenças sociais mais amplas.

A normalização do comportamento sexual online

A alteração das normas culturais relacionadas com a partilha de imagens e interacções sexuais de adultos online está a mudar o panorama. Números elevados de crianças estão a participar na produção de imagens eróticas ou sexuais de si próprias, que podem ser partilhadas mais amplamente ou recolhidas e redistribuídas por pessoas com um interesse sexual em crianças. Nos primeiros seis meses de 2019, o IWF lidou com 22.484 relatórios de material de abuso sexual de crianças autogerado.[100]

A pesquisa da Universidade do Estado de Arizona que envolveu mais de 1.000 estudantes de sete universidades dos EUA indica que o “sexting” (envio de mensagens de natureza sexual) é considerado como parte normal do namoro nos dias de hoje e não se encontra relacionado com comportamento sexual de risco.[101] O IWF descreveu que este comportamento está a ser copiado por crianças e está a começar a ter um papel significativo na vulnerabilidade de vítimas.[102] Os investigadores da INTERPOL confirmaram que este fenómeno cultural não se limita ao Norte Global e tem implicações de protecção complexas em sociedades com fortes tabus culturais e religiosos relacionados com a interacção sexual fora do casamento.[103]

O maior desafio das SGII é que o termo é bastante abrangente e inclui vários comportamentos em que o nível de controlo da criança varia; desde consensual, partilha entre pares dentro de relações adequadas à idade até ao processo coercivo em que adultos (e alguns adolescentes) aliciam, manipulam ou chantageiam uma criança a realizar actividades sexuais através de uma câmara Web para o propósito de obter imagens mais explícitas, partilhando o conteúdo online com outros criminosos.

Concepção de plataformas para a interacção entre adultos e crianças

Em Abril de 2016, dois cidadãos Americanos declararam-se culpados em tribunal relativamente à produção de CSAM e à concepção e operação de dois websites para o propósito de coagir e aliciar menores a partir dos oitos anos a terem condutas sexualmente explícitas através de uma câmara Web. Outros dez membros deste grupo nos Estados Unidos e África do Sul foram acusados e sentenciados.

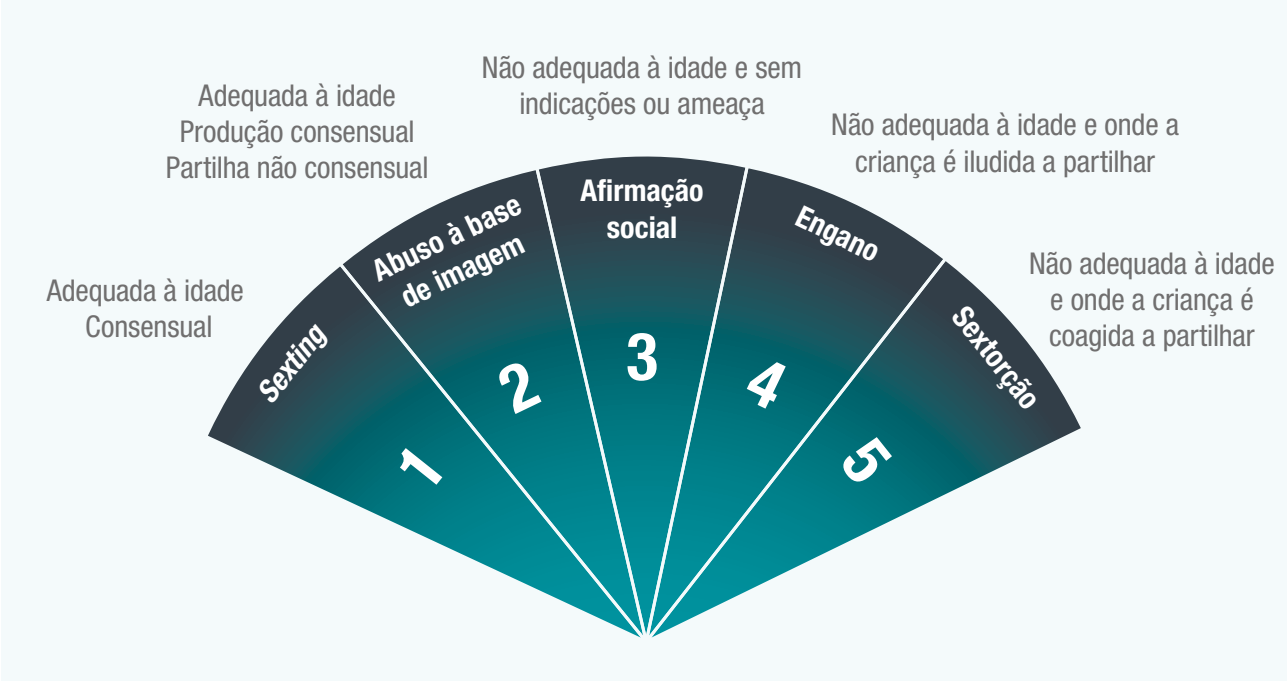
Para aliciar as crianças, criaram perfis falsos nas redes sociais e websites de vídeos populares entre as crianças e utilizaram vídeos pré-gravados de prévias vítimas menores de idade, frequentemente a participar em condutas sexuais explícitas, para convencer as crianças de que estavam a conversar em directo com outro menor.

Estes vídeos coagiram e aliciaram as crianças a participarem em actividades sexualmente explícitas através da sua própria câmara Web, que podia então ser vista por vários membros adultos sem o conhecimento da vítima. Os membros do website atribuíam uma classificação aos esforços uns dos outros para atrair crianças para o website e coagir conduta sexualmente explícita. Estima-se que 1.500 menores foram atraídos para os websites.[104]

Os riscos associados com o abuso e exploração de pares realizados por menores de 18 anos de idade e os riscos associados com este grupo à medida que se tornam adultos também foram identificados como uma ameaça emergente.

Há distintas diferenças relativamente à idade relativa dos participantes, o grau de consentimento/coerção e a intenção criminosa das pessoas que partilham e recebem as imagens. Contudo, há em todos os casos o risco elevado de que SGII e vídeos de crianças sejam obtidos e partilhados online.

Figura 9: Categorização de imagens indecentes autogeradas (Categorisation of self-generated indecent imagery - SGII)



1. **"Sexting"** refere-se à criação e partilha de imagens de natureza sexual, **adequadas à idade e consensuais** , entre dois adolescentes ou jovens, em que se assume haver um certo nível de confiança em como as imagens irão permanecer privadas entre as partes. Há o risco de estas imagens serem partilhadas com outros sem o seu consentimento.
2. **"Abuso com base em imagens"** (também chamado de "imagens indecentes não consensuais" (non-consensual indecent imagery - NCII) refere-se à criação e partilha de imagens de natureza sexual **adequadas à idade** entre dois adolescentes ou jovens, em que as imagens são **partilhadas publicamente sem consentimento**.
3. **"Afirmação social"** refere-se à **transmissão em directo de actos sexuais ou de natureza sexual por parte de crianças** através de uma câmara Web com o objectivo de receber "gosto" e validação. Os sujeitos estão tipicamente fortemente envolvidos, sem a aparente percepção de que a sua conduta representa um encontro sexual danoso.
4. **"Engano"** refere-se aos casos em que a criança é **enganada por um adulto ou adolescente** e acredita que está a participar na produção e partilha consensual de imagens de natureza sexual com pares de idades adequadas. O conspirador alicia as crianças a participarem em actividade sexualmente explícita através das suas próprias câmaras Web, que pode ser vista, sem o consentimento das vítimas, por vários membros adultos com um interesse sexual em crianças. Esta conduta acaba por conduzir, frequentemente, a (5).
5. **"Extorsão sexual"** refere-se ao processo em que adultos ou adolescentes **aliciam, coagem ou manipulam** uma criança a realizar actos sexuais através de uma câmara Web para o propósito de obter mais material explícito para partilhar com outros criminosos. Há um risco de perversidade mais elevado, porque frequentemente o criminoso tem menos medo relativamente ao que poderá fazer com impunidade. A profundidade do trauma da vítima é intensificado por uma sensação de culpa que resultam da chantagem e extorsão.

Tem havido um aumento significativo de SGII nos últimos dois anos, quer produzidas consensualmente, quer como resultado de manipulação ou coacção. Nos primeiros seis meses de 2019, o IWF respondeu a 22.484 relatórios de CSAM online (exactamente um terço de todos os relatórios com que lidaram neste período.[105] Pouco mais de um sexto destas imagens foram categorizadas como enquadrando-se no grupo de gravidade mais elevada (abaixo).

16%	Imagens que envolvem actividade sexual penetrativa e/ou imagens que envolvem actividade sexual com um animal ou sadismo
25%	Imagens que envolvem actividade sexual não penetrativa
58%	Outras imagens indecentes

De entre todos os relatórios, 96% tinham raparigas, 2% tinham rapazes e 2% tinham raparigas e rapazes juntos. Destas imagens, mais de 10% das imagens de raparigas e quase 20% das imagens de rapazes eram de crianças entre os 7 e 10 anos de idade.

Idade	Raparigas (96%)	Rapazes (2%)
Menos de 7 anos	0,7%	4,8%
7-10	10,4%	19,8%
11-13	84,5%	67,7%
Acima de 13 anos	4,4%	7,7%

O número real de sujeitos entre os 13 e 18 anos de idade pode ser mais elevado, uma vez que o IWF não bloqueia imagens se não conseguir determinar se o sujeito tem menos de 18 anos de idade.

Há consequências indesejadas associadas à criminalização dos jovens que partilham imagens de natureza sexual, com o risco de que as sociedades identifiquem acidentalmente crianças a partilhar inapropriadamente imagens de "sexting" como "graves criminosos sexuais", quando na maior parte dos casos o seu "crime" é a ingenuidade. Contudo, o comportamento sexual danoso de jovens é uma área que necessita de muito mais atenção e começa a haver pesquisa a incidir neste grupo, que precisa de apoio e de intervenção terapêutica.

A relação das crianças com a tecnologia é inconstante e tal aumenta o risco

Dois casos no Peru demonstram como a tecnologia tem influenciado a OCSE.

Num dos casos, um criminoso estava a divulgar CSAM com outro indivíduo através das redes sociais. Quando foi preso, confessou que uma mulher lhe tinha enviado o CSAM do Peru. Durante a investigação, os procuradores descobriram o telemóvel da mãe da vítima, que continha fotografias e vídeos em que ela abusava sexualmente de uma das suas filhas e subsequentemente enviava tais materiais por e-mail e por outras redes sociais para um contacto fora do Peru.

Em outro caso, uma criança de 16 anos de idade encontrou um homem de 44 anos de idade através de uma aplicação LGBTQ+. O criminoso pediu ao menor que lhe enviasse fotografias nu e pediu-lhe para ter relações sexuais. Como resultado do seu alto nível de vulnerabilidade, a criança enviou as fotografias e, influenciado pelo criminoso, encontraram-se e tiveram relações sexuais. Após isto, o criminoso assediou a vítima para se encontrarem novamente.[106]

Transmissões de vídeo a pedido

Há indícios de que a Internet está a ser usada não só para facilitar as transacções do tráfico de sexo, como também do tráfico de crianças, especialmente para suprir a procura do cibersexo. Isto é possibilitado pela percepção em algumas culturas de que o cibersexo causa menos danos, porque o abuso é remoto. Um estudo recente de 300 crianças Filipinas que tinham sido abusadas sexualmente online descobriu que a exploração através de uma câmara Web era considerada melhor do que a exploração sexual nas ruas.[107] Os pais que estavam envolvidos em transmissões em directo de OCSE (alguns dos quais eram aliciados pelos criminosos para os introduzir ao cibersexo) acharam que não representavam um risco para as suas crianças, uma vez que não havia nenhum contacto físico directo entre o criminoso e a vítima.

As tendências para o tráfico de cibersexo levaram a solicitações para separar o tráfico de sexo de crianças do tráfico geral previsto por lei, com respectivas penas mais pesadas devido à dupla natureza do crime.

07 O contexto sócio ambiental

Marcadas diferenças entre o Norte e o Sul Global estão a criar uma discordância global preocupante

Os factores ambientais locais podem agravar a vulnerabilidade e fazer com que seja difícil estabelecer parâmetros comuns a nível internacional relativamente ao que constitui abuso, bem como aumentar o desafio de qualquer resposta internacional a nível de protecção de crianças, identificação e detenção de criminosos.

O aumento do acesso à Internet tem aumentado o risco de OCSE em muitos países onde a tecnologia de telemóveis e retransmissão são ainda inovações recentes e onde os recursos de apoio necessários, as orientações de educação e as medidas de protecção para combater a OCSE ainda não amadureceram do ponto de vista técnico. Consequentemente, haverá um número cada vez maior de jovens em nações em desenvolvimento a utilizar a Internet sem consciência dos riscos online a que se sujeitam ou de serviços de apoio disponíveis a nível internacional.

Factores ambientais e educação

Embora os factores socioeconómicos e a desigualdade económica liguem as vítimas às suas vulnerabilidades, como discutido do Capítulo 6, no Norte Global tem havido um investimento significativamente maior para educar as crianças relativamente à segurança online e às relações sexuais. Para além disso, as organizações da sociedade civil são consultadas regularmente sobre políticas governamentais e disponibilizam linhas de ajuda confidenciais para crianças vulneráveis. Contudo, o desenvolvimento tecnológico continua a ser mais rápido do que a capacidade dos governos de apoiar, educar e regular a esfera tecnológica.

Isto acontece de um modo mais visível, se bem que não exclusivo, no Sul Global, onde grandes números de utilizadores estão a adquirir dispositivos e acesso à Internet num contexto em que factores como a pobreza e desigualdade agravam a exposição das crianças à exploração sexual. Por exemplo, a promessa de estabilidade financeira pode incentivar famílias de baixos rendimentos a exporem as suas próprias crianças à exploração e abuso sexual. O colapso do apoio familiar pode fazer com que as crianças acabem por ir viver para a rua, onde a ausência de medidas de protecção e redes de apoio pode aumentar a sua vulnerabilidade relativamente ao tráfico e à exploração sexual em viagens e turismo. Embora as causas da OCSE no mundo em desenvolvimento não tenham sido suficientemente pesquisadas, a UNICEF sugere que a vulnerabilidade das crianças na Internet e fora dela são um reflexo muito próximo uma da outra.[108]

Desmascarar os abusadores

Em 2015, um criminoso Queniano foi sentenciado a prisão perpétua por participar no website de OCSE Dreamboard. O criminoso admitiu ter publicado 121 mensagens no website — um portal de anúncios privado online só para membros que promovia a OCSE e encorajava o abuso e exploração sexual de crianças muito jovens num ambiente concebido para evitar a detecção das autoridades de aplicação da lei. O criminoso era considerado um membro “Super VIP” do Dreamboard, uma designação dada a membros com proeminência no website e que produziam o seu próprio CSAM.

O processo resultou da operação DELEGO, uma investigação lançada em Dezembro de 2009 que visava indivíduos espalhados pelo mundo devido à sua participação no Dreamboard. Um total de 72 indivíduos em cinco continentes diferentes foram alvo de processos penais como resultado. Até à presente data, 49 criminosos declararam-se culpados ou foram condenados após o julgamento. As penas variaram entre cinco anos e prisão perpétua.[109]

Definir, regular e legislar a OCSE

Embora os recursos de educação e apoio ajudem a criar consciencialização digital entre crianças e famílias a nível nacional, os esforços internacionais de combate à OCSE são limitados por uma terminologia de base e regulamentos e legislação de apoio inadequadas.

A Convenção sobre os Direitos da Criança (1989) e o Protocolo Facultativo à Convenção sobre os Direitos da Criança relativo à Venda de Crianças, Prostituição Infantil e Pornografia Infantil (OPSC, 2000) são os instrumentos legais mais pormenorizados a nível internacional que promovem e salvaguardam os direitos da criança e protegem as famílias da venda, exploração sexual e abuso sexual. Contudo, estes tratados foram adoptados numa altura em que as tecnologias de comunicação e serviços de Internet estavam muito menos desenvolvidos e menos generalizados e em que os crimes sexuais contra crianças não tinham os laços estreitos com o ambiente digital que são prevalentes nos dias de hoje.

A 30 de Maio de 2019, o Comité dos Direitos da Criança das Nações Unidas adoptou o seu primeiro Protocolo Opcional de sempre relativo às Orientações sobre a Venda de Crianças, Prostituição Infantil e Pornografia Infantil (OPSC), com o objectivo de facilitar aos estados-nações compreender o que é esperado deles relativamente aos termos de implementação e cumprimento.[110]

O único tratado regional a abordar pormenorizadamente como os estados-nações devem evitar os crimes sexuais contra crianças, julgar os criminosos e proteger as vítimas infantis é a Convenção do Conselho da Europa para a Protecção das Crianças contra a Exploração e os Abusos Sexuais, conhecida por Convenção de Lanzarote.[111] Os seus padrões têm inspirado mudanças na legislação e políticas em países de todo o mundo. Incluem a Directiva da UE relativa à luta contra o abuso sexual e a exploração sexual, que fornece um quadro legislativo holístico que abrange as definições dos crimes, a investigação e processo penal, prevenção e assistência às vítimas.[112] A Convenção de Lanzarote também inspirou a Corte Interamericana de Direitos Humanos que estabeleceu jurisprudência importante relativa à protecção de crianças e o Comité de Peritos Africanos sobre os Direitos e o Bem-estar da Criança, que desenvolveu experiência e competências especializadas para lidar com assuntos importantes, tais como a venda de crianças e o casamento infantil.[113]

No entanto, o facto de haver definições inconsistentes a nível global dificultam o consenso a nível internacional sobre em que consiste a OCSE. Subsequentemente, a divergência regulamentar e legislativa tem criado omissões que permitem aos criminosos evadir as autoridades de aplicação da lei e explorar crianças vulneráveis.

Os desafios de provar que há exploração para remover as imagens

O Gabinete do Comissário de Segurança Electrónica Australiano (*eSafety Commissioner's Office*) realçou que uma pesquisa da Internet pelo nome legal de um dos criminosos, juntamente com o pseudónimo de CSAM da sua filha, revela imagens que são recortes do seu rosto de material de abuso em que ela figura. Contudo, é difícil fazer com que tais imagens sejam removidas, uma vez que as imagens recortadas não mostram abuso sexual.

A tendência recente de as crianças colocarem vídeos delas próprias a dançar no YouTube tornou-se popular com criminosos, que deixaram comentários referindo-se às partes dos vídeos que achavam mais excitantes. O algoritmo do serviço começou subsequentemente a produzir listas de reprodução deste conteúdo e a promovê-lo aos criminosos.

A linha nacional do Canadá para denunciar a OCSE descobriu que necessitam de provar que a imagem é de uma criança e não o contrário. Se houver alguma dúvida de que uma imagem possa ser de um adulto (o que é normal para crianças com mais de 13 anos), torna-se especialmente difícil fazer com que sejam removidas.[114]

Diferenças na legislação internacional

As definições dos crimes variam significativamente entre países. Os crimes relacionados com CSAM estão normalmente (mas não exclusivamente) definidos claramente em países com altos níveis de uso da Internet e levam em consideração os crimes facultados pela Internet. Contudo, em países com um historial relativamente recente de adopção da Internet, as definições legais são frequentemente débeis. Por exemplo, à data de 2018, o CSAM não se encontrava definido na Bósnia-Herzegovina, China, Indonésia, Líbano, Peru, Arábia Saudita, Singapura ou Vietname, isto para referir apenas alguns.[115]

Pesquisa recente do ICMEC a comparar padrões legislativos por todo o mundo com o seu modelo legislativo nacional descobriu que, embora 118 países tivessem legislação suficiente para combater o CSAM, a força de tal legislação varia de país para país.[116]

O ICMEC analisa o progresso da legislação sobre o CSAM em todos os países a nível mundial a cada dois anos e fornece conceitos a serem considerados durante a concepção de legislação para combater o CSAM.

Os critérios principais do relatório permitem avaliar se a legislação nacional:

1. existe especificamente com relação ao CSAM;
2. contém uma definição de CSAM;
3. criminaliza os crimes relacionados com o CSAM facilitados pela tecnologia;
4. criminaliza a posse consciente de CSAM, independentemente da distribuição através da Internet;
5. obriga os prestadores de serviços de Internet (*Internet Service Providers* - ISP) a denunciar suspeitas de CSAM às autoridades de aplicação da lei ou a alguma outra agência responsável.

O relatório de 2018[117] demonstra que:

Número de países	Critérios
118	países têm legislação suficiente para combater os crimes de CSAM (cumprem, pelo menos, quatro dos cinco critérios)
21	países cumprem todos os cinco critérios
16	países não têm qualquer legislação que lide especificamente com o CSAM
51	países não definem o que constitui CSAM
25	países não prevêem crimes de CSAM facilitados por tecnologia
38	países não criminalizam a posse consciente de CSAM, independentemente da intenção de distribuição

A disparidade é agravada por uma tendência identificada de sentenças mais lenientes para criminosos online em países do lado da procura (que dirigem e causam o abuso ou exploração sexual em directo ao instruir e pagar pessoalmente os criminosos que violam as crianças) relativamente aos criminosos que cometem o abuso de contacto "pessoalmente".

Um relatório do programa das Filipinas *International Justice Mission* realça que esta tendência aparenta:

- comprometer a gravidade de crimes de CSEA graves, repetidos e por vezes violentos
- não proporcionar justiça às vítimas vulneráveis, incluindo de países pobres do mundo em desenvolvimento
- não detêm suficientemente estes criminosos
- ser menos eficaz a dissuadir os criminosos de um modo geral.[118]

Os criminosos online representam as mentes e o dinheiro por detrás do abuso de contacto pessoal e devem ser punidos, detidos e dissuadidos em conformidade; em termos práticos, eles estão a promover o abuso de contacto e a cometê-lo por delegação e, assim sendo, são responsáveis pelo crime que ocorreu. Os criminosos do "lado da procura" dirigem e causam o abuso ou exploração sexual em directo ao instruir e pagar pessoalmente aos criminosos que violam as crianças de idades específicas, de modos específicos. Produzem CSAM de cada vez que dirigem e vêem o abuso em directo remotamente e assediam, solicitam e coagem menores a criarem vídeos e imagens sexualmente explícitas para consumo e distribuição.

Contudo, não são só os países com baixos níveis de uso de Internet que têm dificuldades em definir precisamente o que constitui o CSAM. Mesmo em países com leis robustas, os procuradores enfrentam dificuldades a definir de modo adequado e consistente penas para crimes combinados (tais como o assédio, transmissões em directo, partilha de CSAM e chantagem); e, com a Internet a dificultar a distinção entre danos físicos e online, pode acabar por permitir que os criminosos evadam a lei. Por exemplo, antes de se poder abrir um processo penal, as leis de assédio existentes na maior parte dos países requerem que a comunicação seja seguida de uma reunião ou de um plano claro para um encontro com a criança, apesar de um número crescente de casos de assédio online, em que os criminosos aparentam não ter qualquer intenção de se encontrarem pessoalmente.[119] Em vez disso, o objectivo é receber e enviar SGII. Embora a produção, posse e distribuição de tal material seja ilegal, há lacunas que permitem a partilha de capturas de ecrã do conteúdo, mesmo após o original ter sido identificado e removido da Internet.[120]

Combate dos criminosos através da aplicação da lei a nível multinacional

Em 2018, como resultado de uma investigação multinacional da INTERPOL, do Departamento para a Segurança Interna dos EUA e das autoridades da Tailândia e Austrália, nove criminosos foram presos por utilizarem e facilitarem o funcionamento de um portal com CSAM na Web obscura.

O portal tinha 63.000 utilizadores espalhados pelo mundo e continha abuso de mais de 100 crianças, a mais nova com 15 meses. Apesar de grandes esforços para permanecerem anónimos, os investigadores conseguiram localizar e identificar os criminosos.

O administrador principal do portal abusou do sobrinho de forma a fazer contribuições para o portal e, consequentemente, foi sentenciado a 146 anos de prisão. Outro criminoso, que também era um administrador do portal e um professor pré-primário, recebeu uma sentença de 40 anos de prisão, o que representou um recorde na Austrália para crimes de CSAM. Desde o início da operação, pelo menos 50 crianças foram identificadas e salvas de abuso, continuando em curso vários esforços para identificar e salvar mais destas crianças.[121,122]

Uma proposta de uma definição de base

A INTERPOL está a liderar esforços a nível internacional para estabelecer uma definição "de base" da OCSE, com base em critérios que seriam considerados irrefutáveis por todas as nações. [123]Os critérios propostos são os seguintes:

- A vítima é uma criança real;
- A vítima é pré-púbere ou revela os primeiros sinais de puberdade (tipicamente, com menos de 13 anos de idade);
- As imagens demonstram o seguinte:
  - Actividade sexual da criança, com a criança, na presença de uma criança, entre crianças; ou
  - Concentra-se na vagina, pénis ou região anal da criança; e
- A imagem é verificada por vários especialistas em países diferentes.

Regulação de danos online

Nas nações do Norte Global, os governos, as autoridades de aplicação da lei, a indústria tecnológica e o sector terciário cooperam cada vez mais no sentido de encontrar soluções inovadoras para mitigar a divulgação dos danos online.

Tem havido evolução em certos países, incluindo na Austrália, Alemanha e Reino Unido, no reforço da segurança online através da introdução de normas mais rigorosas para a Internet. O Comissariado de Segurança Electrónica Australiano (eSafety Commissioner), criado em 2015, é o regulador, educador e coordenador de segurança online estabelecido, que abrange vários danos. Em Abril de 2018, os EUA promulgaram uma lei conhecida por "FOSTA", que modificou a Lei relativa à Decência nas Comunicações (*Communications Decency Act*) para isentar os prestadores de serviços da imunidade à responsabilização da Secção 230, por publicarem informações fornecidas por terceiros relativas a serviços que se saiba facilitarem ou apoiarem o tráfico sexual.[124] Para além disso, a UE anunciou que irá rever a alteração da imunidade equivalente prevista na Directiva relativa ao comércio electrónico.[125] Contudo, a Internet não se encontra limitada por fronteiras nacionais ou sistemas jurídicos. O desafio consiste em conceber um novo quadro regulamentar para combater um problema global que não tem normas ou definições acordadas a nível internacional.

Em Abril de 2019, o governo do Reino Unido publicou um Livro Branco que propunha estabelecer um órgão nacional para regular conteúdo danoso e tornar o Reino Unido no pais mais seguro do mundo para se utilizar a Internet.[126] Em Julho, após uma cimeira de dois dias relacionada com ameaças correntes e emergentes para a segurança nacional e global, ministros seniores do Reino Unido, Austrália, Canadá, Nova Zelândia e dos Estados Unidos reafirmaram o seu compromisso de trabalhar juntos com a indústria para combater várias ameaças a nível da segurança, incluindo a OCSE. Durante uma mesa-redonda com as empresas de tecnologia, os ministros realçaram que os esforços das agências de aplicação da lei para investigar e abrir processos jurídicos relativamente aos crimes mais graves seriam prejudicados se a indústria continuasse com os planos de implementar a cifragem de ponta a ponta sem as salvaguardas necessárias.[127]

A dicotomia das normas jurídicas

Embora países com normas jurídicas pouco robustas proporcionem mais oportunidades para os criminosos explorarem crianças vulneráveis, países com normas jurídicas robustas e infra-estruturas modernas são responsáveis pelo alojamento de uma percentagem significativa do CSAM online, incluindo os Países Baixos e os EUA, que são os dois países principais em que o CSAM é alojado para audiências globais. A implementação rigorosa de medidas de privacidade de dados em nações com normas jurídicas robustas tem permitido o alojamento Web seguro de CSAM.

Já se tornou evidente que o requisito de remover barreiras do acesso das autoridades de aplicação da lei a comunicações privadas colide com preocupações relacionadas com a privacidade global na Internet. O IWF alertou que solicitar aos ISP que monitorizem activamente as suas redes à procura de conteúdo ilícito entra em conflito directo com o artigo 15.° da Directiva relativa ao comércio electrónico da União Europeia.[128] Actualmente, as empresas privadas não têm o dever legal de partilhar dados sobre o abuso realizado ou denunciado nas suas plataformas, nem sobre as medidas que tomaram para proteger as crianças envolvidas.

A crescente frustração do público com o papel dos ISP como potenciadores de uma vasta gama de danos online irá provavelmente resultar numa análise pormenorizada das normas de privacidade de dados durante a próxima década. As decisões políticas que aumentam a cifragem e o anonimato terão um impacto crucial na OCSE e na nossa capacidade de a combater.

A cooperação internacional é essencial para combater o aumento da gravidade, da escala e da complexidade dos crimes

Em 2019, 337 pessoas foram presas em 38 países, incluindo o Reino Unido, EUA, Irlanda, Coreia do Sul, Alemanha, Espanha, Arábia Saudita, Emirados Árabes Unidos, República Checa e Canadá em conexão com um portal da Web obscura chamado "Welcome to Video".

Este portal era gerido por um criminoso de 23 anos da Coreia do Sul e continha mais de 250.000 vídeos de abuso. Os utilizadores descarregaram mais de um milhão de transmissões de CSAM. O portal comercializava o abuso sexual de crianças e foi um dos primeiros a oferecer vídeos de abuso grave para venda através da criptomoeda Bitcoin. O portal foi desactivado por um grupo de trabalho internacional liderado pela NCA, que incluía o Departamento de Segurança Interna e o Departamento de Investigação Penal do Serviço de Finanças dos Estados Unidos, a polícia nacional da Coreia do Sul e a polícia criminal federal Alemã.

Nikki Holland, a Directora de Investigações da NCA, disse o seguinte: "Os criminosos de sexo infantil da Web obscura, alguns dos quais são os criminosos mais graves, não se conseguem esconder das autoridades de aplicação da lei. Não estão tão escondidos como pensam que estão, não estão tão seguros como pensam que estão."

O caso ilustra o que as autoridades de aplicação da lei têm vindo a constatar relativamente aos crimes sexuais de crianças: o aumento da gravidade, escala e complexidade, incluindo uma ligação directa entre a visualização das imagens de abuso e o abuso de contacto, bem como a utilização da Web obscura e cifragem por parte dos criminosos para esconder as suas actividades e identidades.[129]

08 A amplitude dos danos

O trauma associado ao abuso online tem um impacto negativo enorme e cada vez mais para a vida inteira das vítimas, famílias e sociedade

As quatro lentes de tendências tecnológicas a nível global, ameaça de criminosos, vulnerabilidade de vítimas e o contexto socioeconómico convergem numa quinta lente: os danos.

O trauma associado ao abuso online tem um impacto negativo enorme e cada vez mais para a vida inteira das vítimas e suas famílias, juntamente com os custos para a sociedade de fornecer tratamento médico, cuidados sociais e apoio de saúde mental. A OCSE tem sido associada a problemas com a saúde mental numa idade mais avançada, depressão, um risco mais elevado de toxicodependência e graves problemas de comportamento. O impacto verifica-se não só nas vítimas, mas também no círculo familiar e sistemas sociais/nacionais de saúde e de apoio.

Um estudo de 2017 do Instituto Nacional da Justiça dos Estados Unidos (*National Institute of Justice* - NIJ) constatou que crianças com um historial de abuso físico e emocional tinham uma maior probabilidade de exibir problemas de comportamento durante o meio da infância, o que poderia resultar em comportamento criminoso na idade adulta. Os efeitos parecem ser diferentes nas raparigas e nos rapazes. As primeiras têm tendência para internalizar os problemas, que se manifestam como ansiedade, depressão, isolamento social, enquanto que os rapazes e jovens têm tendência para externalizar os problemas, revelando uma maior hostilidade, agressão e delinquência. Já foi demonstrado que ambos estes tipos de comportamento levam a comportamento criminoso na idade adulta e estão relacionados com perspectivas de educação, emprego, produtividade e financeiras.[130]

Há desafios específicos em países que, por motivos legais e socioculturais, vítimas de abuso sexual do sexo masculino são marginalizadas pela sociedade e/ou lei, ou não se acredita nelas ou não são ajudadas mesmo quando denunciam abuso.

O custo da exploração sexual online de crianças:

De acordo com a Rede de Prevenção de Crimes Sexuais Finlandesa, cada crime sexual acarreta um custo de €15.000 em cuidados médicos e terapia para a vítima.[131] A Europol indicou que esta é uma estimativa bastante conservadora, uma vez que não inclui os custos ao longo da vida causados pelos danos. Contudo, durante o mesmo período de três anos, a terapia preventiva para o criminoso custa €9.600.

O custo para um período de três anos de um crime de natureza sexual contra uma criança	
Custos de investigação preliminar	€3.000
Custos do sistema judicial	€5.000
Pena de prisão entre 2 a 5 anos	€121.600
Custo do programa “STOP” na prisão	€4.300
Custos médicos da vítima	€5.500
Custos de terapia para a vítima para um período de três anos	€9.600
TOTAL	**€149.000**
Custo da terapia preventiva para um período de três anos	€9.600

Um estudo académico avaliou o custo económico para a vida toda resultante do abuso sexual nas crianças nos EUA em, aproximadamente, 9,3 mil milhões de dólares, incluindo os custos associados à despesa governamental e perdas de produtividade.[132]

Jürgen Stock, Secretário Geral da INTERPOL, disse que: *"A escala deste crime é gritante e é agravada pelo facto de que estas imagens podem ser partilhadas online a nível global apenas com o toque de um botão e podem existir para sempre. De cada vez que uma imagem ou vídeo é partilhada ou visualizada, a criança está a ser novamente vitimada."*[133]

A história da Olivia, como relatada no Relatório Anual da Fundação de Observação da Internet de 2018, descreve de um modo integral o trauma e revitimização, uma vez que as imagens do seu abuso infelizmente permaneceram em circulação.

A história da Olivia: o impacto continuado do abuso

Com três anos de idade, a Olivia devia ter estado a brincar com brinquedos, a desfrutar de uma infância inocente. Em vez disso, ela sofreu abusos sexuais horrendos durante vários anos e foi repetidamente violada e torturada sexualmente.

A polícia salvou a Olivia quando tinha cinco anos de idade. Embora o abuso físico tenha terminado, e o homem que a privou da sua infância tenha sido preso, as imagens continuam em circulação e os criminosos continuam a partilhar, e provavelmente a lucrar, da miséria da Olivia. Desde que foi salva, a imagem da Olivia apareceu online cinco vezes em cada dia útil.

Sabemos, de conversar com as pessoas que sofreram de revitimização, que é uma tortura mental que pode destruir vidas e fazer com que seja difícil deixar o abuso no passado.

A consciência de que uma imagem do sofrimento destas vítimas está a ser partilhada ou vendida online já é muito difícil para as mesmas. Mas, para as pessoas sobreviventes, o medo de serem identificadas ou reconhecidas na idade adulta é aterrador.[134]

Outro desafio cada vez maior consiste no medo que a vítima tem de divulgar o que se está a passar com ela ou, em alguns casos devido à sua idade muito jovem, a uma falta de entendimento do que é errado, possivelmente como resultado de o abuso ter sido cometido por um criminoso dentro do círculo familiar ou numa posição de confiança. Podem haver vários factores que contribuem para isso, incluindo o medo de que não se acredite nelas, o medo da permanência — de que as imagens e as respectivas mensagens permaneçam online para sempre e sentimentos de vergonha, constrangimento e culpa. Marie Collins, a fundadora da Fundação Marie Collins e uma vítima de abuso sexual em criança, falou exaustivamente sobre estes sentimentos: *"Como criança, não teria falado com ninguém sobre o meu abuso, porque se tivesse falado com alguém sobre as imagens essa pessoa poderia encontrá-las. Eu não queria de todo que ninguém as encontrasse, porque iriam ver como eu era uma pessoa terrível… mas estava sempre preocupada com essas imagens… onde estavam e quem as tinha visto."*[135]

Este medo de permanência é real e a revitimização é uma consideração relativamente recente que é amplificada pelo abuso online. As imagens continuam a circular durante anos após o período de abuso original, mesmo depois de a vítima ter sido salva e de o criminoso ter sido preso e julgado.

Em reconhecimento de que a primeira geração de vítimas de imagens de abuso sexual infantil que foi distribuído online está a atingir a idade adulta, a Pesquisa aos Sobreviventes a Nível Internacional do Centro Canadiano para a Protecção de Menores está a procurar compreender melhor os impactos deste crime e determinar que alterações políticas, legislativas e terapêuticas são necessárias para responder às necessidades destas vítimas.[136]

O Phoenix 11

O Phoenix 11 é um grupo de onze sobreviventes cujo abuso sexual infantil foi gravado e, na maior parte dos casos, distribuído online. O Phoenix 11 foi criado com o objectivo de ser uma força poderosa para combater as respostas inadequadas à prevalência das imagens de abuso sexual infantil online na Internet.

Em Fevereiro de 2018, o Centro Canadiano para a Protecção de Menores (*Canadian Centre for Child Protection*), juntamente com o Centro Nacional para as Crianças Desaparecidas e Exploradas (*National Center for Missing and Exploited Children* - NCMEC) dos EUA, organizou o primeiro retiro para este grupo único de sobreviventes na América do Norte. O propósito era fornecer um local em que os sobreviventes pudessem partilhar alguns dos desafios com que se deparam, ou com que se depararam, num ambiente seguro e de mútuo apoio, para criar laços e promover relações com outros sobreviventes. Um dos resultados foi a criação de um grupo de advocacia, o Phoenix 11, com o objectivo de se concentrar a trazer a voz colectiva das vítimas e dos sobreviventes ao plano internacional para criar mudanças.

O Centro Canadiano assiste e apoia os esforços do Phoenix 11 na defesa da necessidade de mudanças ao escrever cartas em seu nome, ao facilitar o uso da sua Declaração de Impacto Comunitário em processos jurídicos e ao solicitar que forneçam feedback em materiais educativos e de outra natureza que se destinam a audiências externas.[137]

A tecnologia também é uma oportunidade para parar o abuso

Num mundo em que um número cada vez maior de crianças tem contas nas redes sociais e passa uma quantidade de tempo cada vez maior do seu tempo online, a questão de como os proteger assume uma importância fundamental. Embora os governos tenham a responsabilidade de promulgar leis e implementar políticas nas suas jurisdições, não têm capacidade de combater esta batalha sozinhos. As empresas do sector privado, as comunidades locais, organizações a desenvolver tecnologia para identificar e remover conteúdo e os media têm todos um papel crucial.

O relatório do Grupo de Trabalho Técnico da Aliança para a Dignidade da Criança inclui uma recomendação de que a indústria deve ser vivamente encorajada, ou mesmo obrigada através de legislação doméstica, a:

- ser obrigada a analisar as suas redes, plataformas e serviços, ou tomar medidas semelhantes, como um procedimento operacional automático, para detectar CSAM conhecido, incluindo os serviços “de passagem” (conhecidos por “passthrough”).
- aplicar normas e códigos de conduta contra comportamento ilegal nas suas plataformas
- implementar redes, códigos de prática e padrões mínimos em que a segurança é integrada na concepção (safety by design).[138]

Revitimização

Em Agosto de 2019, um denunciante do sexo masculino e outro do sexo feminino contactaram a Fundação Aarambh, que aloja o portal de denúncia do IWF na índia, com URL de conteúdo de vídeo dos próprios quando eram crianças. A aflição das vítimas com a emergência do conteúdo online das suas infâncias, bem como o estigma social ao seu redor, teve um efeito directo nas suas vidas, incluindo no seu emprego, casamento e actividades sociais. Ao rever denúncias das autoridades de aplicação da lei na Índia, as organizações foram capazes de verificar as suas idades e certificar-se de que os URL criminosos foram removidos.[139]

Com novos desafios emergentes à medida que as empresas privadas e as plataformas das redes sociais começam a utilizar comunicações mais seguras e cifragem de ponta a ponta, irá haver a necessidade de acção a nível global para garantir que as novas tecnologias podem ser utilizadas na identificação e gestão de conteúdo ilegal e danoso.

A inteligência artificial e a aprendizagem automática estão a ter um papel crucial ao fazer o "trabalho árduo" na detecção de imagens e vídeos danosos em escala. Isto reduz o perigo de revictimização e permite que especialistas com formação concentrem os seus esforços mais eficientemente e dêem prioridade às revizualizações nos locais certos. Contudo, por si só não são a solução. Por exemplo, os modelos de aprendizagem automática da geração actual têm alguma dificuldade a identificar rostos, idades e o género de crianças de grupos étnicos distintos e estas são algumas das lacunas em que a comunidade de tecnologia global devia estar a concentrar-se.

Projecto Arachnid

O Projecto Arachnid é operado pelo Centro Canadiano para a Protecção de Menores e representa uma ferramenta inovadora no combate à proliferação cada vez maior de CSAM na Internet.

A plataforma do Projecto Arachnid foi inicialmente concebida para navegar ligações para websites que continham CSAM previamente denunciados no Cybertip.ca, para detectar se estas imagens/vídeos estavam a ser disponibilizadas ao público. Se o CSAM fosse detectado, um aviso era enviado ao provedor a fazer o alojamento do conteúdo, a solicitar que fosse removido.

O Projecto Arachnid continua a realizar as actividades de navegação descritas acima, mas está continuamente a desenvolver e a adaptar-se, reforçando as suas capacidades para acelerar a detecção de CSAM e facilitando assim a sua remoção atempada.

Nos primeiros três anos de operação, o Projecto Arachnid teve os seguintes volumes:

- Analisou 2 mil milhões de páginas Web com mais de 91 mil milhões de fotografias Dessas, 13,3 milhões eram suspeitas (ou seja, possível CSAM com base no DNA Fotográfico)
- 4,6 avisos para remover conteúdo foram enviados a provedores
- 85% dos avisos dizem respeito a vítimas que se pensa não terem sido identificadas pela polícia.[140]

09 A perspectiva futura

Com base na nossa avaliação da ameaça, os seguintes são alguns dos passos recomendados que as nações podem tomar individualmente, ou colectivamente, para mitigar o impacto. Pode consultar mais pormenores na Resposta Estratégica Global à Exploração e Abuso Sexual de Crianças Online, disponível no website da Aliança Global WePROTECT: https://www.weprotect.org/

O relatório deste ano demonstra que o rápido crescimento do acesso global à Internet e os dispositivos inteligentes de baixo custo resultam em mais eventuais vítimas e criminosos a aceder à Internet. A facilidade do acesso por parte dos consumidores a serviços de comunicações seguras, com cifragem de ponta a ponta, significa que os criminosos estão cada vez mais bem protegidos nos seus "refúgios digitais seguros", com níveis sem precedentes de cooperação e partilha de informações. Os criminosos têm vários canais para aceder à mesma instância de abuso e o encorajamento dos pares valida e normaliza os comportamentos criminosos.

Embora estes aspectos tecnológicos e sociais promovam a proliferação da criminalidade e aproximem os criminosos das suas vítimas, há factores sociais, culturais e económicos que têm um impacto na amplificação do risco e dos danos. Tem havido um declínio constante na idade das crianças às quais é permitido ter acesso não supervisionado às redes sociais e a jogos multijogador online, bem como uma alteração a nível de comportamento que normaliza a partilha de imagens e o comportamento sexual online.

Os factores importantes que contribuem para combater este problema à sua escala actual são a capacidade do quadro legislativo de cada nação de fornecer uma protecção adequada às crianças; a disponibilidade de agentes de aplicação da lei com altos níveis de formação que possam ser rápida e eficazmente utilizados para combater os criminosos e para localizar e salvaguardar as vítimas; bem como a sua capacidade para envolver e regular a indústria tecnológica no sentido de aplicar medidas de protecção adequadas em linha com as políticas actualizadas. Contudo, não nos devemos esquecer de que a responsabilidade pela OCSE é, em primeiro lugar, dos criminosos.

Hoje, através da Aliança Global WePROTECT, os estados-nação, as autoridades de aplicação da lei, a indústria tecnológica, as instituições académicas e o terceiro sector podem todos tornar-se parte da solução global para este crime hediondo contra as pessoas mais vulneráveis da nossa sociedade.

De forma a combater esta ameaça persistente e em crescimento, eis alguns passos que as nações podem tomar individualmente e as acções que devem fazer em conjunto:

- ✓ **A comunidade internacional** deve prestar mais atenção a programas concebidos para evitar que as pessoas cometam crimes pela primeira vez e que reincidam, tendo em conta os altos custos do apoio terapêutico ao longo da vida para as vítimas, bem como para detectar, abrir processos penais, encarcerar e reabilitar criminosos.
- ✓ **A comunidade internacional** deve utilizar tecnologia e prestadores de serviços a montante mais consistentemente a nível nacional e internacional.
- ✓ **A comunidade internacional** deve considerar mudar o paradigma no modelo actual de notificação e remoção para aliviar as vítimas de trauma e retirar maus repositórios de conteúdo da Internet, ao mesmo tempo que melhoram o acesso internacional e a partilha de dados.
- ✓ **A comunidade internacional** deve continuar com a criação de um regime de classificação de OCSE consistente, analisando as lacunas existentes na legislação para informar a nova política.
- ✓ As**empresas globais de tecnologia** devem ser mais proactivas nos seus esforços para examinar, detectar e remover CSAM e frustrar as tentativas de assédio, abraçando uma metodologia em que a segurança é integrada na concepção (safety by design) e não um modelo passivo em que simplesmente reage à OCSE, por exemplo, através da verificação online das crianças.
- ✓ **As Nações** com competências especializadas em aspectos do Modelo de Resposta Nacional devem ter o dever de o partilhar como outros países (consultar: https://www.weprotect.org/the-model-national-response para mais informações).
- ✓ **As Nações** devem ter como objectivo nomear um líder, educador e regulador nacional para coordenar os esforços de segurança online e para facilitar a remoção de conteúdo nocivo.
- ✓ **As Nações** devem assegurar-se de que as redes de apoio à vítima para a vida toda são adequadamente disponibilizadas e financiadas.
- ✓ **Os decisores políticos a nível nacional** devem procurar ter uma estratégia equilibrada no que diz respeito à segurança, privacidade e legislação de segurança pública, assegurando-se de que a privacidade não invalida ou cancela a habilidade das empresas de tentar identificar proactivamente CSAM ou comportamento de assédio.
- ✓ **Os decisores políticos a nível nacional** devem ter uma estratégia concentrada na vítima, ao conceberem políticas de prevenção e medidas de intervenção, ao trabalharem com agências de média profissionais e ao envolverem as perspectivas das vítimas e as vozes dos jovens.
- ✓ **As agências de aplicação da lei** devem trabalhar em conjunto para aumentar a partilha de tecnologias avançadas e técnicas de investigação inovadoras, para melhorar a identificação das vítimas e combater a OCSE em grande escala.
- ✓ **Os peritos de segurança online** devem partilhar as melhores práticas relativamente a quadros educativos de boas práticas, conteúdo e métodos de ensino, bem como avaliar a sua eficácia na mudança de comportamentos.
- ✓ **Os prestadores de cuidados sociais** devem obter uma melhor compreensão das pessoas mais vulneráveis ou susceptíveis à exploração online e devem desenvolver intervenções personalizadas para os apoiar.

10 Notas de fim

1 "Online Harms White Paper" (Governo Britânico, 3) disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/591512/HO_DfE_consultation_response_on_CSE_definition_FINAL_13_Feb_2017__2_.pdf (consultado a 01 de Outubro de 2019)

2 Aliança Global WeProtect – Avaliação Mundial da Ameaça 2018

3 https://www.justice.gov/opa/pr/kenyan-child-pornography-producer-sentenced-life-prison-participation-dreamboard-website (consultado a 01 de Outubro de 2019)

4 https://www.justice.gov/opa/pr/kenyan-child-pornography-producer-sentenced-life-prison-participation-dreamboard-website (consultado a 01 de Outubro de 2019)

5 "Project Arachnid" (Centro Canadiano para a Protecção de Menores, dados à data de 1 de Novembro de 2019) disponível em: https://projectarachnid.ca/en/#shield)

6 https://www.justice.gov/opa/pr/kenyan-child-pornography-producer-sentenced-life-prison-participation-dreamboard-website (consultado a 01 de Outubro de 2019)

7 Citado em "Internet Organised Crime Threat Assessment" (EUROPOL, 2019: pág. 30)

8 Número citado em "The dark side of the internet for children: online child sexual exploitation in Kenya – A Rapid Assessment Report" (Terre des Hommes, 2018: pág. 3) disponível em: https://www.terredeshommes.nl/sites/tdh/files/uploads/tdh-nl_ocse_in_kenya_research_report_feb_2018.pdf (consultado a 01 de Outubro de 2019)

9 "Internet Organised Crime Threat Assessment" (EUROPOL, 2019: pág. 30)

10 Correspondência da INTERPOL com o PA Consulting Group (2019)

11 "National Strategic Assessment" (National Crime Agency, 2019: pág. 13)

12 "Association of Sexting with Sexual Behaviours and Mental Health Among Adolescents" em Jama Paediatrics (Mori et al, 2019) citado em https://www.huffpost.com/entry/talking-toyour-kid-about-sexting_l_5d408dc8e4b007f9accf9939 (consultado a 01 de Outubro de 2019)

13 Aliança Global WeProtect – Avaliação Mundial da Ameaça 2018

14 Dados relacionados directamente com estudos de caso apresentados aos pesquisadores da PA Consulting pelo EVAC Fund, 15 de Outubro de 2019

15 Dados relacionados directamente com estudos de caso apresentados aos pesquisadores da PA Consulting pelo eSafety Commissioner Australiano, 17 de Outubro de 2019

16 "Global Digital Report 2019: Essential insights into how people around the world use the internet, mobile devices, social media and e-commerce" (We Are Social, 2019: pág. 8), disponível em: https://wearesocial.com/global-digital-report-2019 (consultado a 01 de Outubro de 2019)

17 "Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online", (Broadband Commission: 2019)

18 "Global Digital Report 2019: Essential insights into how people around the world use the internet, mobile devices, social media and e-commerce" (We Are Social, 2019: pág. 8-63)

19 "The State of the World's Children 2017: Children in a Digital World" (UNICEF, 2017: pág. 1)

20 "INHOPE Statistics Report" (INHOPE, 2018: pág. 2)

21 https://www.justice.gov/opa/pr/kenyan-child-pornography-producer-sentenced-life-prison-participation-dreamboard-website (consultado a 11 de Outubro de 2019)

22 "Annual Report 2018" (Fundação de Observação da Internet, 2019)

23 “Global Digital Report 2019: Essential insights into how people around the world use the internet, mobile devices, social media and e-commerce” (We Are Social, 2019: pág. 8-63)

24 “Global Digital Report 2019: Essential insights into how people around the world use the internet, mobile device, social media and E-Commerce”

25 “Global Digital Report 2019: Essential insights into how people around the world use the internet, mobile devices, social media and e-commerce” (We Are Social, 2019: pág. 8)

26 Estimativa atribuída ao Dr. Michael Seto, psicólogo clínico e forense do grupo Royal Ottawa Healthcare, “How many men are paedophiles?” citado em https://www.bbc.co.uk/news/magazine-28526106 (consultado a 01 de Outubro de 2019)

27 “How common is males’ self-reported sexual interest in prepubescent children?” (Dombert et al., 2016) e “The Revised Screening Scale for Pedophilic Interests (SSPI-2): Development and Criterion-Related Validation” (Seto et al. 2015)

28 https://www.justice.gov/opa/pr/kenyan-child-pornography-producer-sentenced-life-prison-participation-dreamboard-website (consultado a 11 de Outubro de 2019)

29 ”Annual Report 2018” (Fundação de Observação da Internet, 2019)

30 Correspondência da INTERPOL com o PA Consulting Group (2019)

31 Aliança Global WeProtect – Avaliação Mundial da Ameaça 2018

32 “National Strategic Assessment” (National Crime Agency, 2019: pág. 13)

33 “Internet Organised Crime Threat Assessment” (EUROPOL, 2018: pág. 32)

34 “Internet Organised Crime Threat Assessment 2019 Report” (EUROPOL), disponível em: https://www.EUROPOL.europa.eu/activities-services/main-reports/internet-organised-crime-threatassessment

35 “The Internet is Overrun with Images of Child Sexual Abuse. What Went Wrong?” (New York Times, 2019) disponível em https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html (consultado a 01 de Outubro de 2019)

36 “Internet Organised Crime Threat Assessment” (EUROPOL, 2018: pág. 32)

37 “Global Digital Report 2019: Essential insights into how people around the world use the internet, mobile devices, social media and e-commerce’ (We Are Social, 2019: pg. 88), disponível em: https://wearesocial.com/globaldigital-report-2019 (consultado a 01 de Outubro de 2019)

38 “Breaking the Dark Net” (VG, 2017) available at https://www.vg.no/spesial/2017/undercover-darkweb/?lang=en (consultado a 01 de Outubro de 2019)

39 “The Top 7 Messenger Apps in the World” (Inc., 2018) disponível em: https://www.inc.com/larrykim/the-top-7-messenger-apps-in-world.html

40 “DNS over HTTPS: Why we’re saying DoH could be catastrophic” (Internet Watch Foundation, 17 de Julho de 2019) available at https://www.iwf.org.uk/news/dns-over-https-whywe%E2%80%99re-saying-doh-could-becatastrophic

41 “Internet Organised Crime Threat Assessment” (EUROPOL, 2018: pág. 33)

42 “Draft Council Conclusions on combating the sexual abuse of children” (Conselho da União Europeia, 2019) available at: https://data.consilium.europa.eu/doc/document/ST-12326-2019-INIT/en/pdf (consultado a 10 de Outubro de 2019)

43 https://www.justice.gov/opa/pr/kenyan-child-pornography-producer-sentenced-life-prison-participation-dreamboard-website (consultado a 29 de Outubro de 2019)

44 "How paedophiles use cookies and keywords to hide sexual abuse images in innocent looking sites" (Independent, 2017) disponível em: https://www.independent.co.uk/life-style/gadgets-and-tech/features/paedophiliachild-sexual-abuse-images-video-codeskeywords-clues-cookies-iwf-maskingbreadcrumbing-a7661051.html (consultado a 01 de Outubro de 2019)

45 Correspondência da INTERPOL com o PA Consulting Group (2019)

46 "Teenage Brides Trafficked to China Reveal Ordeal" (New York Times, 2019) disponível em: https://www.irishtimes.com/news/crime-and-law/virtual-child-abuse-imagery-a-headache-for-garda%C3%AD-1.3803910 (consultado em 01 de Outubro de 2019)

47 "Online Harms White Paper" (Governo Britânico, 2018) disponível em: https://www.theguardian.com/technology/2018/mar/20/child-abuse-imagery-bitcoin-blockchain-illegal-content (consultado a 01 de Outubro de 2019)

48 "Internet Organised Crime Threat Assessment" (EUROPOL, 2019: pág. 33)

49 Correspondência da International Justice Mission com o PA Consulting Group (2019)

50 "Internet Organised Crime Threat Assessment" (EUROPOL, 2019: pág. 35)

51 "Internet Organised Crime Threat Assessment" (EUROPOL, 2019: pág. 32)

52 "Internet Organised Crime Threat Assessment" (EUROPOL, 2019: pág. 37)

53 Mais informação sobre a campanha "Trace an Object" da EUROPOL disponível em: https://www.EUROPOL.europa.eu/stopchildabuse (consultado a 01 de Outubro de 2019)

54 "Online Harms White Paper" (Governo Britânico, 2019) disponível em: https://www.gov.uk/government/news/security-summit-ends-with-pledges-to-tackle-emerging-threats (consultado a 01 de Outubro de 2019)

55 "Etiology of Adult Sexual Offending', in Sex Offender Management and Planning Initiative at the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking" (Faupel, S., and Przybylski, R.) disponível em: https://www.smart.gov/SOMAPI/sec1/ch2_etiology.html (consultado a 01 de Outubro de 2019)

56 "Towards a Global Indicator: On unidentified victims in child sexual abuse material" (INTERPOL, ECPAT, 2018) disponível em https://www.ecpat.org/wp-content/uploads/2018/03/TOWARDS-A-GLOBAL-INDICATOR-ONUNIDENTIFIED-VICTIMS-IN-CHILD-SEXUALEXPLOITATION-MATERIAL-Summary-Report.pdf

57 Base de dados de ICSE da INTERPOL

58 "Mapping Online Child Safety in Asia and the Pacific," em *Asia and the Pacific Policy Studies*, Vol. 5, Número 3, (Singh, R. D., 2018: pág. 651-664)

59 "#SoSockingSimple wins ISPA best PR campaign" (Internet Watch Foundation, 12 de Julho de 2019) disponvel em: https://www.iwf.org.uk/news/sosockingsimple-wins-ispa-best-prcampaign

60 "National Strategic Assessment" (National Crime Agency, 2019: pág. 12)

61 Correspondência da INTERPOL com o PA Consulting Group (2019)

62 "The State of the World's Children 2017: Children in a Digital World" (UNICEF, 2017: pág. 1)

63 Apresentação feita na Conferência "Tackling Online Child Sexual Exploitation" do *Policing Institute for the Eastern Region* (PIER) (Anglia Ruskin University, 25-26 de Abril de 2019) por Marcella Leonard (perita em terapia psicossexual, protecção de crianças e do público) www.leonardconsultancy.co.uk

64 Correspondência da INTERPOL com o PA Consulting Group (2019)

65 Correspondência da INTERPOL com o PA Consulting Group (2019)

66 Correspondência do Ministério da Administração Interna Britânico com o PA Consulting Group (2019)

67 Correspondência da International Justice Mission com o PA Consulting Group (2019)

68 "Child Sexual Abuse Material – Model Legislation and Global Review" (Centro Internacional para as Crianças Desaparecidas e Exploradas, 2018) disponível em: https://www.icmec.org/child-pornography-model-legislation-report/ (consultado em 01 de Outubro de 2019)

69 Correspondência da INTERPOL com o PA Consulting Group (2019)

70 "Online Harms White Paper" (Governo Britânico, 2018) disponível em: https://www.csacentre.org.uk/csa-centre-prod/assets/File/CSE%20perpetrators%202%20-%20Characteristics%20and%20motivations%20of%20perpetrators%20of%20CSE.pdf (consultado a 01 de Outubro de 2019)

71 "INTERPOL network identifies 10,000 child sexual abuse victims" (INTERPOL, 2017) disponível em: https://www.basw.co.uk/system/files/resources/basw_64920-4.pdf (consultado a 01 de Outubro de 2019)

72 "A review of the evidence for female sex abusers" (McCloskey & Raphael, 2005), cited in 'Who Abuses Children?' (Australian Government Institute of Family Studies CFCA Resource Sheet, 2014) available at: https://aifs.gov.au/cfca/publications/who-abuses-children (accessed 01 October 2019)

73 Dados NCMEC, fornecidos pela INTERPOL, 05 de Setembro de 2019

74 "INTERPOL network identifies 10,000 child sexual abuse victims" (INTERPOL, 2018) disponível em: https://www.iwf.org.uk/news/iwf-global-figures-show-online-child-sexual-abuse-imagery-up-by-a-third (consultado a 19 de Outubro de 2019)

75 "INTERPOL network identifies 10,000 child sexual abuse victims" (INTERPOL, 2019) disponível em: https://supchina.com/2019/07/24/china-vows-to-take-a-hardline-on-child-sexual-abuse/ (consultado a 01 de Outubro de 2019)

76 "Online Harms White Paper" (Governo Britânico, 2019) disponível em: https://www.chinadailyhk.com/articles/233/225/172/1542599418213.html (consultado a 01 de Outubro de 2019)

77 Correspondência do Fundo para Pôr Termo à Violência Contra Crianças (End Violence Against Children - EVAC) com o Secretariado da WeProtect Global Alliance e o PA Consulting Group (2019)

78 Correspondência do Fundo para Pôr Termo à Violência Contra Crianças (End Violence Against Children - EVAC) com o Secretariado da WeProtect Global Alliance e o PA Consulting Group (2019)

79 1"Child sexual abuse images on the internet: a cybertip.ca analysis" (Canadian Centre for Child Protection, 2016) disponível em: https://www.protectchildren.ca/pdfs/CTIP_CSAResearchReport_2016_en.pdf (consultado a 01 de Outubro de 2019)

80 Correspondência do Fundo para Pôr Termo à Violência Contra Crianças (End Violence Against Children - EVAC) com o Secretariado da WeProtect Global Alliance e o PA Consulting Group (2019)

81 "The State of the World's Children 2017: Children in a Digital World" (UNICEF, 2017: pág. 1)

82 "How safe are our children?" (NSPCC, 2019)

83 Números citados em "Studies in Child Protection: Technology-Facilitated Child Sex Trafficking" (Centro Internacional para as Crianças Desaparecidas e Exploradas, 2018: pág. 10)

84 Números citados em "Studies in Child Protection: Technology-Facilitated Child Sex Trafficking" (Centro Internacional para as Crianças Desaparecidas e Exploradas, 2018: pág. 10)

85 Números citados em “Studies in Child Protection: Technology-Facilitated Child Sex Trafficking” (Centro Internacional para as Crianças Desaparecidas e Exploradas, 2018: pág. 10)

86 “Fortnite Frenzy Key Findings” (Common Sense Media, 2018) disponível em: https://www.commonsensemedia.org/fortnite-frenzy-key-findings (consultado a 01 de Outubro de 2019)

87 Correspondência do Ministério da Administração Interna Britânico com o PA Consulting Group (2019)

88 “Sexual Exploitation of Children in Cambodia Submission for the Universal Periodical Review of the human rights situation in Cambodia” (APLE Cambodia, ECPAT International 2018)

89 Número citado em “The dark side of the internet for children: online child sexual exploitation in Kenya – A Rapid Assessment Report” (Terre des Hommes, 2018: pág. 6) disponível em: https://www.terredeshommes.nl/sites/tdh/files/uploads/tdh-nl_ocse_in_kenya_research_report_feb_2018.pdf (consultado a 01 de Outubro de 2019)

90 Número citado em “The dark side of the internet for children: online child sexual exploitation in Kenya – A Rapid Assessment Report” (Terre des Hommes, 2018: pág. 11) disponível em: https://www.terredeshommes.nl/sites/tdh/files/uploads/tdh-nl_ocse_in_kenya_research_report_feb_2018.pdf (consultado a 01 de Outubro de 2019)

91 “Sexual Exploitation of Children in Cambodia Submission for the Universal Periodical Review of the human rights situation in Cambodia” (APLE Cambodia, ECPAT International 2018: pg. 4)

92 https://projectarachnid.ca/en/#faq (consultado a 03 de Novembro de 2019)

93 “Understanding African Children’s use of ICT; A youth-lead survey to prevent sexual exploitation Online”, (ECPAT International, 2013) citado em “The dark side of the internet for children: online child sexual exploitation in Kenya – A Rapid Assessment Report” (Terre des Hommes, 2018)

94 Citado em “Sexual Exploitation of Children in Mexico Submission for the Universal Periodic Review of the Human Rights Situation in Mexico” (ECPAT Mexico, 2018) disponível em: https://www.ecpat.org/wp-content/uploads/2018/07/Universal-Periodical-Review-Sexual-Exploitation-of-Children-Mexico.pdf (consultado a 01 de Outubro de 2019)

95 “How safe are our children?” (NSPCC, 2019: pág. 13)

96 “We keep it in our hearts: sexual violence against men and boys in the Syria crisis” (ACNUR, Relatório de outubro de 2017)

97 “Teenage Brides Trafficked to China Reveal Ordeal” (New York Times, 2019) disponível em: https://www.nytimes.com/2019/08/17/world/asia/china-bride-trafficking.html (consultado em 01 de Outubro de 2019)

98 “Sex Slaves: The Prostitution, Cybersex & Forced Marriage of North Korean Women & Girls in China” (Korea Future Initiative, 2019) disponível em https://www.koreafuture.org/report/sex-slaves (consultado a 01 de Outubro de 2019)

99 “Korean Approaches to Online Protection for Children in Digital Era” (Jalil, J., 2013) citado em “Global study on sexual exploitation of children in travel and tourism” (ECPAT International, 2016: pg. 27) disponível em: https://www.protectingchildrenintourism.org/wp-content/uploads/2018/10/Global-Report-Offenders-on-the-Move.pdf (consultado a 01 de Outubro 2019)

100 1”Child sexual abuse images on the internet: a cybertip.ca analysis” (Canadian Centre for Child Protection, 2016) disponível em: https://www.protectchildren.ca/pdfs/CTIP_CSAResearchReport_2016_en.pdf (consultado a 01 de Outubro de 2019)

101 Instruções do IWF aos investigadores da PA Consulting, 27 de Setembro de 2019

102 Pesquisa realizada por Johnstonbaugh, M., Arizona State University, citada em "Sexting is a normal part of modern dating", (Daily Mail, 2019) disponível em: https://www.dailymail.co.uk/sciencetech/article-7363601/Sexting-normal-modern-dating-NOT-associated-sexually-risky-behavior.html (consultado em 01 de Outubro de 2019)

103 Instruções do IWF aos investigadores da PA Consulting, 27 de Setembro de 2019

104 Instruções da INTERPOL aos investigadores da WePROTECT Secretariat E PA Consulting, 05 de Setembro de 2019

105 https://www.justice.gov/opa/pr/members-international-child-exploitation-conspiracy-plead-guilty (consultado a 15 de Outubro de 2019)

106 Correspondência da Fundação de Observação da Internet com o PA Consulting Group (2019)

107 Correspondência do Fundo para Pôr Termo à Violência Contra Crianças (End Violence Against Children - EVAC) com o PA Consulting Group (2019)

108 "The dark side of the internet for children: online child sexual exploitation in Kenya – A Rapid Assessment Report" (Terre des Hommes, 2018: pg. 14) disponível em: https://www.terredeshommes.nl/sites/tdh/files/uploads/tdh-nl_ocse_in_kenya_research_report_feb_2018.pdf (consultado a 01 de Outubro de 2019)

109 "The State of the World's Children 2017: Children in a Digital World" (UNICEF, 2017)

110 https://www.justice.gov/opa/pr/kenyan-child-pornography-producer-sentenced-life-prison-participation-dreamboard-website (consultado a 15 de Outubro de 2019)

111 "Explanatory Report to the Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography" (ECPAT International, 2019)

112 "Convenção do Conselho da Europa para a Proteção das Crianças contra a Exploração e os Abusos Sexuais ('a Convenção de Lanzarote')" (Conselho da Europa, 2007)

113 "Directiva 2011/93/UE relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil" disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093 (consultada a 03 de Novembro de 2019)

114 "Terminology Guidelines: For the protection of children from sexual exploitation and sexual abuse" (Grupode trabalho interagências no Luxemburgo, 2016)

115 Correspondência do Gabinete do Comissário de Segurança Electrónica Australiano com o PA Consulting Group (2019)

116 "Child Sexual Abuse Material – Model Legislation and Global Review" (Centro Internacional para as Crianças Desaparecidas e Exploradas, 2018) disponível em: https://www.icmec.org/child-pornography-model-legislation-report/ (consultado em 01 de Outubro de 2019)

117 "Child Sexual Abuse Material – Model Legislation and Global Review" (Centro Internacional para as Crianças Desaparecidas e Exploradas, 2018) disponível em: https://www.icmec.org/child-pornography-model-legislation-report/ (consultado em 01 de Outubro de 2019)

118 "Child Sexual Abuse Material – Model Legislation and Global Review" (Centro Internacional para as Crianças Desaparecidas e Exploradas, 2018) disponível em: https://www.icmec.org/child-pornography-model-legislation-report/ (consultado em 01 de Outubro de 2019)

119 Correspondência da International Justice Mission com o PA Consulting Group (2019)

120 "Child Sexual Abuse Material – Model Legislation and Global Review" (Centro Internacional para as Crianças Desaparecidas e Exploradas, 2018) disponível em: https://www.icmec.org/child-pornography-model-legislation-report/ (consultado em 01 de Outubro de 2019)

121 "Trends in Online Child Sexual Exploitation: Examining the distribution of Captures of Live-streamed Child Sexual Abuse" (Internet Watch Foundation, 2018)

122 “50 children rescued, 9 sex offenders arrested in international operation” (INTERPOL, 2019) disponível em: https://www.INTERPOL.int/en/News-and-Events/News/2019/50-children-rescued-9-sex-offenders-arrested-in-international-operation (consultado a 20 de Outubro de 2019)

123 “Fifty children saved as international paedophile ring busted” (BBC, 2019) disponível em: https://www.bbc.co.uk/news/world-48379983 (consultado a 20 de Outubro de 2019)

124 Correspondência da INTERPOL com o PA Consulting Group (2019)

125 A Lei relativa ao Combate do Tráfico de Sexo Online (The Fight Online Sex Trafficking Act - FOSTA) e Lei para Parar de Capacitar os Traficantes de Sexo (Stop Enabling Sex Traffickers Act - SESTA) entraram em vigor nos EUA a 11 de Abril de 2018

126 “US, Europe threatens tech industry’s cherished legal ‘shield’’ (Politico, 2018) disponível em: https://www.politico.eu/article/tech-platforms-copyright-e-commerce-us-europe-threaten-tech-industrys-cherished-legal-shield/ (consultado a 20 de Outubro de 2019)

127 “Online Harms White Paper” (Governo Britânico, 2019) disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf (consultado a 20 de Outubro de 2019)

128 “Five Country Ministerial communiqué: emerging threats, London 2019” (Governo Britânico, 2019) disponível em: https://www.gov.uk/government/publications/five-country-ministerial-communique/five-country-ministerial-ommunique-emerging-threats-london-2019 (consultado a 20 de Outubro de 2019)

129 “Online Harms White Paper Response” (Fundação de Observação da Internet, 2019: pág. 9)

130 “337 arrested after takedown of horrific dark web child abuse site Welcome To Video” (NCA, 2019) disponível em: https://nationalcrimeagency.gov.uk/news/337-arrested-after-takedown-of-horrific-dark-web-child-abuse-site-welcome-to-video (consultado a 21 de Outubro de 2019)

131 ”Effects of Child Maltreatment, Cumulative Victimization Experiences, and Proximal Life Stresses on Adult Crime and Antisocial Behaviour” (Herrenkohl, T. I. et al., 2017)

132 “Preventing Sexual Crimes”, citado em “New and Innovative ways to tackle child sexual abuse” (Save the Children)

133 “The economic burden of child sexual abuse in the United States” (Letourneau, E. J., et al., 2018: pág. 413-22)

134 “INTERPOL network identifies 10,000 child sexual abuse victims” (INTERPOL, 2017) disponível em: https://www.INTERPOL.int/en/News-and-Events/News/2017/INTERPOL-network-identifies-10-000-child-sexual-abuse-victims (consultado a 20 de Outubro de 2019)

135 ”Annual Report 2018” (Fundação de Observação da Internet, 2019)

136 Citado em “Digital dangers: The impact of technology on the sexual abuse and exploitation of children and young people” (Barnardo’s and Marie Collins Foundation, 2016: pág. 37)

137 ”International Survivors’ Survey” (Centro Canadiano para a Protecção de Menores, Setembro de 2017), disponível em: https://www.protectchildren.ca/en/resources-research/survivors-survey-results/

138 ”Phoenix 11” (Centro Canadiano para a Protecção de Menores) disponível em: https://protectchildren.ca/en/programs-and-initiatives/phoenix11/)

139 Correspondência da Fundação Aarambh com o PA Consulting Group (2019)

140 “Project Arachnid” (Centro Canadiano para a Protecção de Menores, dados à data de 1 de Novembro de 2019) disponível em: https://projectarachnid.ca/en/#shield)

Mais informações

Pode consultar mais informações no nosso website
www.weprotect.org

ou siga-nos no Twitter @weprotect