



AVALIAÇÃO DA AMEAÇA GLOBAL 2021

Trabalhamos juntos para erradicar
o abuso sexual de crianças online



Conteúdo

- 01** Prefácio
- 02** Sumário executivo
- 03** Introdução
- 04** Estimativas sobre a exposição aos danos sexuais online na infância, e respetivos fatores de risco – resumo das conclusões
- 05** Temas:
 - COVID-19
 - Tecnologia
 - Regulação, cooperação voluntária e transparência
- 06** Danos:
 - Aliciamento online de crianças para fins de abuso e exploração sexual
 - Produção de material de abuso sexual de crianças
 - Pesquisa por e/ou visualização de material de exploração e abuso sexual de crianças
 - Partilha e/ou retenção de material de abuso sexual de crianças
 - Material sexual "autogerado" pelas crianças
 - Streaming ao vivo de situações de exploração e abuso sexual de crianças
- 07** Recomendações
- 08** Agradecimentos
- 09** Glossário
- 10** Anexo A: Inquérito WeProtect Global Alliance/Technology Coalition sobre as empresas tecnológicas
- 11** Notas finais

Prefácio

Sejam bem-vindos à 3ª Avaliação da Ameaça Global pela WeProtect Global Alliance – sendo que é a primeira realizada desde o nosso lançamento enquanto entidade independente em abril de 2020.

Desde então, a COVID-19 vem registrando um impacto sem precedentes no modo de vida das populações. O mundo online tornou-se mais importante do que nunca na vida dos mais jovens. Para que possamos proteger eficientemente as crianças da exploração e do abuso sexual online, precisamos em primeiro lugar, de entender o problema com que nos deparamos. Para tal, precisámos de ouvir desde os governos ao setor privado, passando pela sociedade civil e — o mais importante — as vítimas e sobreviventes deste tipo de agressão.

Pela primeira vez, entrevistámos milhares de jovens adultos no mundo inteiro sobre as suas vivências de danos sexuais online. Nesta avaliação, partilhamos as descobertas exclusivas relativas ao setor das tecnologias e a resposta do mesmo a este tipo de crime, tendo igualmente reunido as informações recolhidas junto das empresas de segurança online acerca das tendências emergentes. Tudo isto, articulado com uma resposta sem precedentes por parte dos nossos membros, possibilitou que esta nossa avaliação fosse a mais abrangente e alargada de sempre.

Vemo-nos hoje confrontados com três insights principais:

- 1 A escala da exploração sexual e do abuso de crianças online é crescente — um crescimento sustentado que já ultrapassa a nossa capacidade de resposta global. A luta contra o abuso sexual de crianças mantém-se como cronicamente subfinanciada. Por essa razão, temos vindo a trabalhar com tanto afinco no sentido de construir esta Aliança Global. Todos concordamos — todos os 98 governos, 53 empresas, 61 organizações da sociedade civil e nove instituições internacionais — que o abuso sexual de crianças online é inaceitável. E todos concordamos que precisamos colaborar para acabar com esta situação. O que sabemos agora é que tal exige uma mudança radical na nossa resposta global.
- 2 A prevenção precisa de ser uma prioridade na nossa resposta. Demasiadas vezes ficamos à espera que o abuso aconteça para encetarmos qualquer ação. É essencial uma aplicação musculada da lei e da resposta judicial. Contudo, para que a estratégia seja verdadeiramente sustentável, é necessário prevenir o abuso, de forma ativa — o que passa por algo mais do que apenas a promoção da segurança online das crianças. Será necessário mais do que a Safety by Design e outras iniciativas que dificultam a exploração dos serviços online pelos infratores. Será necessário mais do que a simples dissuasão dos potenciais infratores. Prevenir será necessariamente tudo isto e muito mais.

Precisamos de garantir que estamos a criar ambientes seguros online, onde as crianças possam crescer em segurança e desenvolver as suas competências. Este trabalho promissor já está em andamento, mas necessita de maior suporte.

- 3 A esperança existe. Na última década, o abuso e exploração sexual de crianças online ganharam relevo na agenda global. Hoje há mais países, mais empresas e mais organizações da sociedade civil que estão envolvidas no combate a este crime. A tecnologia de segurança online tornou-se mais acessível e avançada. Os governos estão a clarificar e a reforçar as responsabilidades dos prestadores de serviços online na prevenção e a sua abordagem ao abuso sexual de crianças nas suas plataformas. A mudança pode estar a avançar a um ritmo mais lento do aquilo que desejaríamos, mas está a acontecer. O nosso papel enquanto Global Alliance é alimentar estas iniciativas nascentes e ajudá-las a crescer.

Por último, gostaríamos de agradecer às entidades PA Consulting, Crisp, Economist Impact, ao Steering Committee dedicado ao projeto, assim como a todos os que contribuíram, quer sejam nossos membros ou não, para tornar este documento uma realidade. A vossa visão, os desafios conquistados e a dedicação foram inestimáveis. Estamos convencidos de que as futuras Avaliações da Ameaça Global contarão a história de como a colaboração de todos e o engenho vêm possibilitando a resolução deste problema e garantindo que as crianças de todo o mundo podem desfrutar dos benefícios de um mundo digital livre da ameaça do abuso e da exploração sexual.



Iain Drennan
Administrador Executivo
WeProtect Global Alliance



Ernie Allen
Presidente
WeProtect Global Alliance

02

Sumário Executivo

As crianças enfrentam hoje uma ameaça constante de exploração e abuso sexual online.

A nossa resposta global a este crime precisa de uma nova abordagem, caso contrário um número ainda mais elevado de crianças vai continuar a correr riscos e a sofrer o trauma deste tipo de abuso.

A melhor estratégia para a mudança é o melhoria da segurança online para as crianças aliada à redução de oportunidades para os infratores.

De forma consistente com as Avaliações de Ameaças Globais anteriores, este relatório revela que a exploração e o abuso sexual de crianças online continuam a proliferar. **Muitas das tendências emergentes ameaçam aumentar o volume e a complexidade dos casos** e a exacerbar os desafios para aqueles que trabalham na redução dos riscos e danos.

Este relatório destaca também as oportunidades para reforçar a resposta com base numa abordagem com múltiplas camadas. Todos têm um papel a desempenhar, desde os reguladores, às organizações da sociedade civil, ao setor da tecnologia e às autoridades judiciais e policiais.

Figura 1: A escala do desafio





Ao descrevermos a rápida diversificação dos danos associados à ameaça, analisamos igualmente as causas da exploração e do abuso sexual de crianças. A tecnologia encontra-se atualmente integrada em todos os aspetos da vida quotidiana. Apesar disso, continuamos a diferenciar falsamente o tratamento que fazemos daquilo que é o abuso "online" (em oposição a "presencial"), o que é patente na condenação em sentenças mais leves para os crimes "online".⁵ Tal revela claramente que a nossa resposta não tem conseguido acompanhar a ameaça.

Desde a Avaliação da Ameaça Global de 2019, a natureza dos danos continuou a crescer e a diversificar-se.

Nos últimos dois anos, as denúncias de exploração e abuso sexual de crianças online atingiram o nível mais elevado. As evidências indicam um aumento:

- Na incidência do aliciamento online.^{6 7}
- No volume de material de abuso sexual de crianças disponível online.⁸
- Na partilha e distribuição de material de abuso sexual de crianças.⁹
- Na transmissão de streaming ao vivo mediante pagamento.¹⁰

A escala e a taxa de evolução não têm precedentes, conforme ilustram os dados do US National Center for Missing and Exploited Children (NCMEC —Centro Nacional para Crianças Desaparecidas e Exploradas dos Estados Unidos) e da Internet Watch Foundation (IWF).

+100%

Aumento das denúncias efetuadas pelo público relativamente a situações de exploração sexual online, (NCMEC) ¹¹

De 2019 a 2020.

77%

Aumento do material sexual "autogerado" pela criança, (IWF) ¹²

De 2019 a 2020.

A pandemia COVID-19 tem vindo a ser, inegavelmente, um fator que contribui para o aumento da exploração e do abuso sexual de crianças online (ver Capítulo Tema: COVID-19). O aumento do material sexual "autogerado" por crianças é outra tendência que desafia a resposta existente.

O aumento de denúncias pode não equivaler a um aumento proporcional das instâncias do crime: algumas podem provir do aumento da consciencialização pública e da deteção mais proativa por parte dos prestadores de serviços online. Contudo, os níveis de abuso podem ser mais graves do que os sugeridos pelos dados disponíveis:

- 1 A exploração e o abuso sexual de crianças são crimes sub-reportados.¹³ Num inquérito global da Economist Impact, 54% dos inquiridos afirmaram ter sofrido danos sexuais online durante a infância, incluindo terem-lhes sido enviados conteúdos sexualmente explícitos, bem como ter-lhes sido pedido que fizessem algo com que se sentiam desconfortáveis.

Existem relativamente menos dados disponíveis sobre a escala do problema nos países do Hemisfério Sul (ver Glossário de Termos). É possível que as taxas de abuso e exploração estimadas venham a ser revistas em alta à medida que essa lacuna de evidências seja resolvida.

- 2 Ao passo que a maioria das empresas que responderam à pesquisa WeProtect Global Alliance/Technology Coalition utilizam ferramentas para detetar material de abuso sexual de crianças (são usadas ferramentas de "hash-matching" de imagem e vídeo por 87% e 76%, respetivamente), apenas 37% utilizam ferramentas para detetar o aliciamento online. Isto sugere que uma proporção significativa dessa atividade pode não estar a ser detetada.¹⁴

Até mesmo os abusadores com competências técnicas mínimas conseguem evadir a deteção utilizando serviços de mensagens encriptadas que são facilmente acessíveis, bem como ferramentas de anonimato. No outro extremo da escala, conforme destacado pela Crisp, alguns infratores da Dark Web (ver Glossário) utilizam técnicas avançadas para ofuscar as suas atividades. A utilização de "serviços ocultos" para distribuir material de abuso sexual de crianças aumentou 155% de 2019 para 2020.¹⁵ Em geral, é possível que a deteção dos casos seja reduzida, especialmente nas jurisdições em que a capacidade de investigação digital é limitada.

As tendências recentes têm o potencial de alimentar o crescimento sustentado da criminalidade:

- As novas formas de monetização do material de abuso sexual de crianças bem como o crescimento do conteúdo "autogerado" pelas mesmas, em troca de pagamento, reforçam as motivações comerciais para o abuso.
- O aumento do volume de materiais "autogerados" por crianças está a criar desafios complexos aos legisladores.
- Os abusadores estão a diversificar os seus métodos de produção, por exemplo, coagindo as crianças a praticarem atos sexuais que são captados ilicitamente em vídeo ("capping"). O Centro Australiano de Combate à Exploração Infantil (Australian Centre to Counter Child Exploitation) relata que o "capping" gera aproximadamente 60-70% das referências apresentadas à Unidade de Identificação de Vítima.¹⁶

O presente relatório ajuda a construir uma imagem mais precisa do comportamento dos abusadores. O estereótipo predominante de "estranho perigoso" não é corroborado pelas evidências. O abuso sexual de menores é frequentemente perpetrado por membros da família,^{17 18 19 20} e existem indicadores de que o fenómeno se exacerbou face às restrições da COVID-19. Adicionalmente, ainda que alguns criminosos sejam motivados pelo interesse sexual por crianças, esse não é o único cenário. De acordo com a Fundação Lucy Faithfull, apenas 15% a 20% dos abusadores que vêm sendo estudados atualmente, são pedófilos para os quais "as crianças pré-púberes constituem o principal interesse sexual".²¹ É fundamental continuarmos a melhorar a nossa compreensão das várias ramificações deste tipo de abuso, de modo a desenvolvermos futuras formas de dissuasão e prevenção.

É fundamental continuarmos a melhorar a nossa compreensão das várias ramificações deste tipo de abuso, de modo a desenvolvermos futuras formas de dissuasão e prevenção.

Esta Avaliação da Ameaça Global destaca áreas de foco prioritárias e oportunidades emergentes para deter o crescimento da exploração sexual e do abuso de crianças online.

A Global Strategic Response (GSR) da WeProtect Global Alliance apresenta uma estratégia global abrangente para eliminar a exploração e o abuso sexual de crianças.²²

Esta Avaliação da Ameaça Global identifica quatro áreas de foco dentro quadro de resposta:

Área de foco/opportunidade recomendada:	Regulação da Internet
Categoria GSR:	Políticas/Legislação
<p>Alguns países têm evoluído nas suas respostas legislativas, produzindo leis que responsabilizam legalmente os prestadores de serviços online.</p> <p>A regulação da Internet tem o potencial de tornar os ambientes online mais seguros para as crianças. É necessário criar quadros legais de apoio desenvolvidos e consultadoria criteriosa para garantir que os resultados pretendidos são alcançados.</p>	

Área de foco/opportunidade recomendada	Fomento da capacidade das autoridades policiais e judiciais
Categoria GSR:	Justiça Criminal
<p>Ainda que alguns países beneficiem de respostas legais avançadas, as diversas autoridades policiais enfrentam dificuldades fundamentais que as impedem de acompanhar a ameaça. Grande parte das forças de segurança é subfinanciada, carece do equipamento necessário e é ultrapassada pela dimensão da atividade criminosa.</p> <p>Os governos terão de aumentar o investimento nas forças policiais. Só assim será possível melhorar a capacidade do policiamento digital de cada país, permitindo uma melhor colaboração e cooperação no que concerne aos crimes transnacionais e tecnicamente sofisticados através da criação de unidades multinacionais especializadas de investigação criminal.</p>	

Área de foco/opportunidade recomendada	Cooperação voluntária, transparência e tecnologias de segurança online.
Categoria GSR:	Tecnologia
<p>A criação de complementos poderosos à regulamentação, cooperação voluntária e transparência permite criar a capacidade de resposta necessária para enfrentar uma ameaça em rápida evolução.</p> <p>Desde a Avaliação da Ameaça Global de 2019 que têm sido dados passos significativos no sentido de influenciar as plataformas digitais a cumprirem os princípios de "Safety by Design" e de estimular o investimento global em tecnologias de segurança online. Com as estruturas de suporte certas a funcionar, e uma implementação mais generalizada, estas soluções têm potencial para aumentar significativamente a resposta geral às ameaças.</p>	

Área de foco/opportunidade recomendada:	Iniciativas sociais (diversas)
Categoria GSR:	Social
<p>É necessário criar um foco renovado numa série de iniciativas sociais, incluindo:</p> <ul style="list-style-type: none"> • Intervenções destinadas a formar os jovens no sentido de desenvolverem comportamentos sexuais saudáveis. • Iniciativas que incidam sobre a raiz do problema da exploração e do abuso sexual de crianças, como por exemplo, a atitude face às mulheres — uma recente Revisão das Evidências da UNICEF concluiu que “o indicador mais forte de atitudes de aceitação do abuso sexual de crianças são (...) as opiniões que apoiam a supremacia masculina relativamente às mulheres²³. • Intervenções sociais no sentido de reduzir os estigmas que impedem quer a denúncia dos abusos quer a obtenção de ajuda por parte daqueles que estão em risco de cometer abusos. 	

A exploração e o abuso sexual de crianças online são algumas das questões mais prementes e determinantes da nossa geração.

Estas áreas de foco recomendadas têm o potencial de impedir a ocorrência da exploração e do abuso sexual de crianças — ou a sua recidiva. Em termos gerais, prevenção significa:

Redução dorisco de prevaricação, identificando aqueles em risco de cometer crimes, ajudando-os a lidar com comportamentos problemáticos, e também por meio de uma apertada gestão de risco dos criminosos já condenados.

Redução do risco para as crianças. Criação de ambientes mais seguros para as crianças. O ônus da responsabilidade não deverá recair sobre as crianças no sentido de reduzir o risco de ser alvo de abusos.

Redução do risco geral, neutralizando os fatores estruturais que propiciam o abuso. Uma prevenção eficaz abarca intervenções sociais que combatam a raiz da exploração e do abuso sexual de crianças.

A prevenção representa o melhor caminho para garantir a sustentabilidade das respostas futuras.

Isto deve estar lado a lado com o papel dos serviços da linha de frente na resposta aos casos, na interrupção dos abusadores e no apoio às vítimas e aos sobreviventes. A chave está em equilibrar o investimento na prevenção enquanto parte de todo um sistema de resposta integrada.

Juntos, temos o conhecimento, os meios e a oportunidade de agir, de melhorar a resposta global e de evitar que mais crianças sejam prejudicadas.

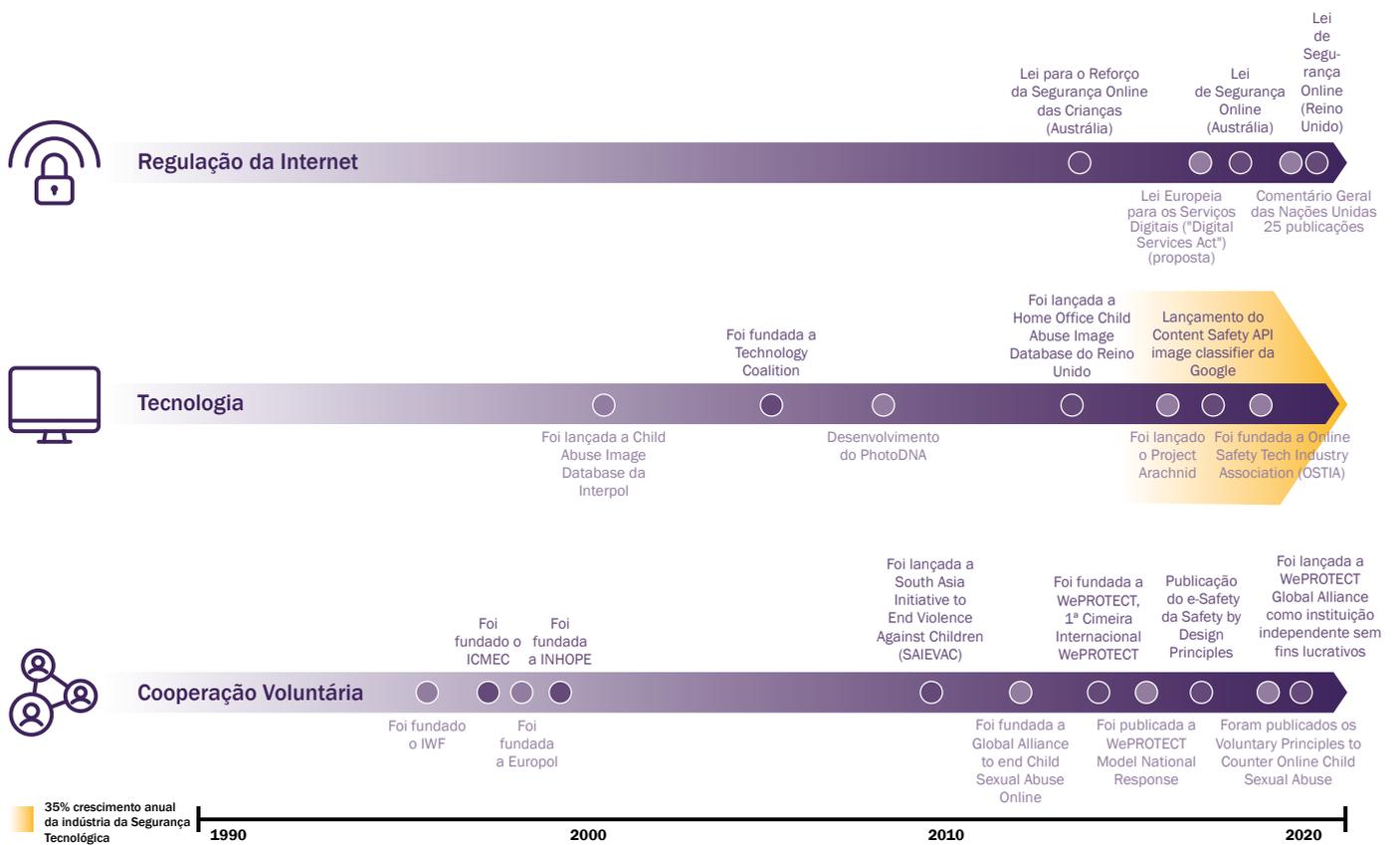
A exploração sexual e o abuso de crianças online são uma das questões mais prementes e determinantes da nossa geração. Cada país enfrenta desafios diferentes, encontrando-

se em diferentes estágios no desenvolvimento das respectivas respostas às ameaças. Alguns países registaram uma rápida aceleração da conectividade à Internet nos últimos anos, sendo que a consciência social relativamente aos danos online é ainda relativamente incipiente. Já em outros países, existe uma exigência mais coerente por parte do consumidor no clamar por uma gestão proativa desta questão.

Assoluções de tecnologia implementadas pelos prestadores de serviços online trazem benefícios globais, bem como as abordagens legislativas locais que incentivam as empresas multinacionais a melhorarem os índices de transparência, responsabilidade e capacidade de resposta geral. A Figura 2 ilustra os principais desenvolvimentos das últimas três décadas que impulsionaram a resposta internacional à exploração e abuso sexual de crianças online. É provável que o impulsionamento desses desenvolvimentos se mantenha à medida que os serviços online evoluem e que os consumidores, em todo o mundo, se tornam mais conscientes — e menos tolerantes — relativamente aos danos decorrentes. As principais recomendações emergentes da Avaliação da Ameaça Global deste ano estão detalhadas no Capítulo 7:

Recomendações. Embora as medidas devam ser adaptadas e priorizadas de acordo com os contextos locais, estas são ações que podem ser implementadas por todas as empresas, comunidades e governos no sentido de melhorar a resposta ao problema da exploração e abuso sexual de crianças online. Todos temos a responsabilidade global partilhada de trabalhar de forma concertada para manter as crianças a salvo do perigo — em 2021 temos uma oportunidade sem precedentes para o conseguir, ao apoiar o impulso global de transformação da nossa resposta coletiva.

Figura 2: Mapeamento de alguns dos principais desenvolvimentos relacionados com os fatores capacitadores de uma resposta preventiva melhorada.



Introdução

DEFINIÇÕES-CHAVE

Abuso sexual de crianças é "o envolvimento de uma criança [pessoa menor de 18 anos] em atividade sexual que ela não compreende totalmente, é incapaz de dar consentimento informado ou para a qual não está preparada em termos da sua maturidade e não pode dar o seu consentimento". Esta é a definição de abuso sexual de crianças adotada pela WeProtect Global Alliance ("a Aliança"), com base nas²⁴ diretrizes da Organização Mundial da Saúde (OMS).

Exploração sexual infantil é uma forma de abuso sexual sobre crianças que envolva qualquer forma tentada ou efetiva de abuso de uma posição de vulnerabilidade, diferencial de poder ou de confiança. Isto inclui, entre outros, a busca do lucro monetário, social ou político através do ato de exploração sexual de outra pessoa. Pode ser perpetrado por indivíduos ou grupos de abusadores. O que distingue a exploração sexual infantil do abuso sexual de crianças é a noção subjacente da interação presente na exploração.²⁵ Existe uma significativa sobreposição entre os dois conceitos, porque a exploração costuma ser uma característica do abuso e vice-versa.²⁶

A exploração e o abuso de crianças online são parcial ou totalmente facilitados pela tecnologia, ou seja, através da Internet e/ou outras comunicações sem fios. Este conceito também é conhecido como Online Child Sexual Exploitation and Abuse (sigla em inglês: OCSEA – Exploração e Abuso Sexual de Crianças Online) e exploração e abuso sexual de crianças "facilitados pela tecnologia".



Âmbito

Este relatório constitui a terceira Avaliação da Ameaça Global publicada pela Aliança para delinear a escala e a abrangência da exploração e abuso sexual de crianças online e para galvanizar uma resposta.

A Avaliação da Ameaça Global 2019 concluiu que as tendências emergentes sinalizavam um "tsunami" no crescimento dos eventos de exploração e abuso sexual de crianças online, "deixando um rastro cada vez maior de vítimas e sobreviventes à sua passagem".²⁷ A Avaliação de 2019 focou-se na análise da ameaça através de quatro lentes principais: as vítimas, os abusadores, as tendências tecnológicas e o contexto socioeconómico.

Este relatório adota uma abordagem "baseada nos danos causados" de modo a permitir uma exploração mais estratificada das diferenças nas experiências das vítimas e dos sobreviventes, dos métodos dos abusadores, das tecnologias facilitadoras e dos contextos socioeconómicos das diferentes manifestações da exploração e abuso sexual de crianças online. A definição está patente na Figura 3: Definições de danos. Esta abordagem permite uma avaliação mais completa dos fatores concorrentes para cada dano e das oportunidades de intervenção assim como das estratégias de resposta.

Os danos examinados estão interligados, conforme ilustrado na Figura 4 e seguintes.

Examinamos, ainda, três temas transversais:

- COVID-19.
- Tecnologia.
- Regulação, Cooperação Voluntária e Transparência.

NOTA NA TERMINOLOGIA DOS DANOS

Os "danos" (definidos na Figura 3) são descrições de abusos cometidos por perpetradores. Estas não foram redigidas para refletir as experiências das vítimas e dos sobreviventes. Destinam-se a explorar os fatores ligados ao crime: onde reside o ónus principal para a interrupção e a prevenção da atividade criminosa. Esta terminologia não tem a intenção de diminuir o impacto sobre as vítimas, que também é explorado relativamente a cada dano, inclusivamente nos correspondentes estudos de caso.

Figura 3: Definições de Danos

Danos	Definição
<p>Aliciamento online de crianças com vista à sua exploração e abuso sexual</p>	<p>Uma pessoa constrói uma relação de confiança e conexão emocional com uma criança ou jovem com o intuito de a manipular, explorar e abusar sexualmente (de forma facilitada, parcial ou totalmente, pela Internet ou outras comunicações sem fios).²⁸ Nem sempre existe a intenção de encontro presencial.</p> <p><i>Nota: Algumas organizações usam o termo alternativo "preparação online" (conforme definido pelo NCMEC²⁹) para se referir a este tipo de dano.</i></p>
<p>Produção de materiais de abuso sexual de crianças</p>	<p>Criação de material de abuso sexual de crianças (consulte o Glossário) presencialmente através fotografia/vídeo/registo áudio; criação de conteúdo textual ou não fotográfico (por exemplo, gerado por computador); ou manipulação de material visual já existente de abuso sexual de crianças para criar imagens novas.</p>
<p>Pesquisa por e/ou visualização de material de exploração e abuso sexual de crianças</p>	<p>Busca por material de abuso sexual de crianças na Internet e visualização ou tentativa de visualização do mesmo.</p>
<p>Partilha e/ou retenção de material de abuso sexual de crianças</p>	<p>Download, partilha e/ou retenção de material de abuso sexual de crianças</p>
<p>Material sexual "autogerado" pela criança</p>	<p>Conteúdo de natureza sexual, incluindo imagens e vídeos de nudez total ou parcial, produzidos pelas próprias crianças. O material sexual "autogerado" por crianças não constitui um dano por si mesmo (pode ser produzido voluntariamente e partilhado como parte de uma troca adequada para a idade e o estágio de desenvolvimento como seja, por exemplo, entre adolescentes). No entanto, existem situações em que o dano é causado, em primeiro lugar:</p> <ul style="list-style-type: none"> • quando uma criança ou adolescente é coagido a produzir material sexual "autogerado". • Quando o material sexual "autogerado" voluntariamente é partilhado contra a vontade do adolescente. <p>Este relatório examina as características da "autoprodução" nociva. Esta frase aparece entre aspas ao longo do relatório para evitar sugerir vontade por parte da criança ou jovem envolvido. Embora o conteúdo possa atender à definição de material de abuso sexual de crianças, normalmente a intenção não está estabelecida claramente, não podendo ser considerada como tal em circunstância alguma.</p>
<p>Streaming ao vivo de situações de exploração e abuso sexual de crianças</p>	<p>Transmissão em tempo real de situações de exploração e abuso sexual de crianças pela Internet.</p>

Objetivos

O objetivo principal deste relatório é detalhar a escala e a abrangência da ameaça de exploração e abuso sexual de crianças online, com uma avaliação que seja compreensível e significativa para públicos em todo o mundo. Pretende servir de encorajamento a ações baseadas em evidências, reconhecendo o importante progresso alcançado até o momento e destacando as oportunidades de redução do risco para as crianças, bem como prevenir o abuso antes que ele aconteça.

Metodologia

Este relatório é um metaestudo que apura as conclusões de vários estudos internacionais para aumentar o seu alcance global, construir uma imagem holística da ameaça e proporcionar uma avaliação equilibrada sempre que as informações forem incompletas ou existir discordância entre especialistas (referindo as respetivas advertências sempre que adequado).

Esta investigação secundária é apoiada por várias formas de investigação primária :

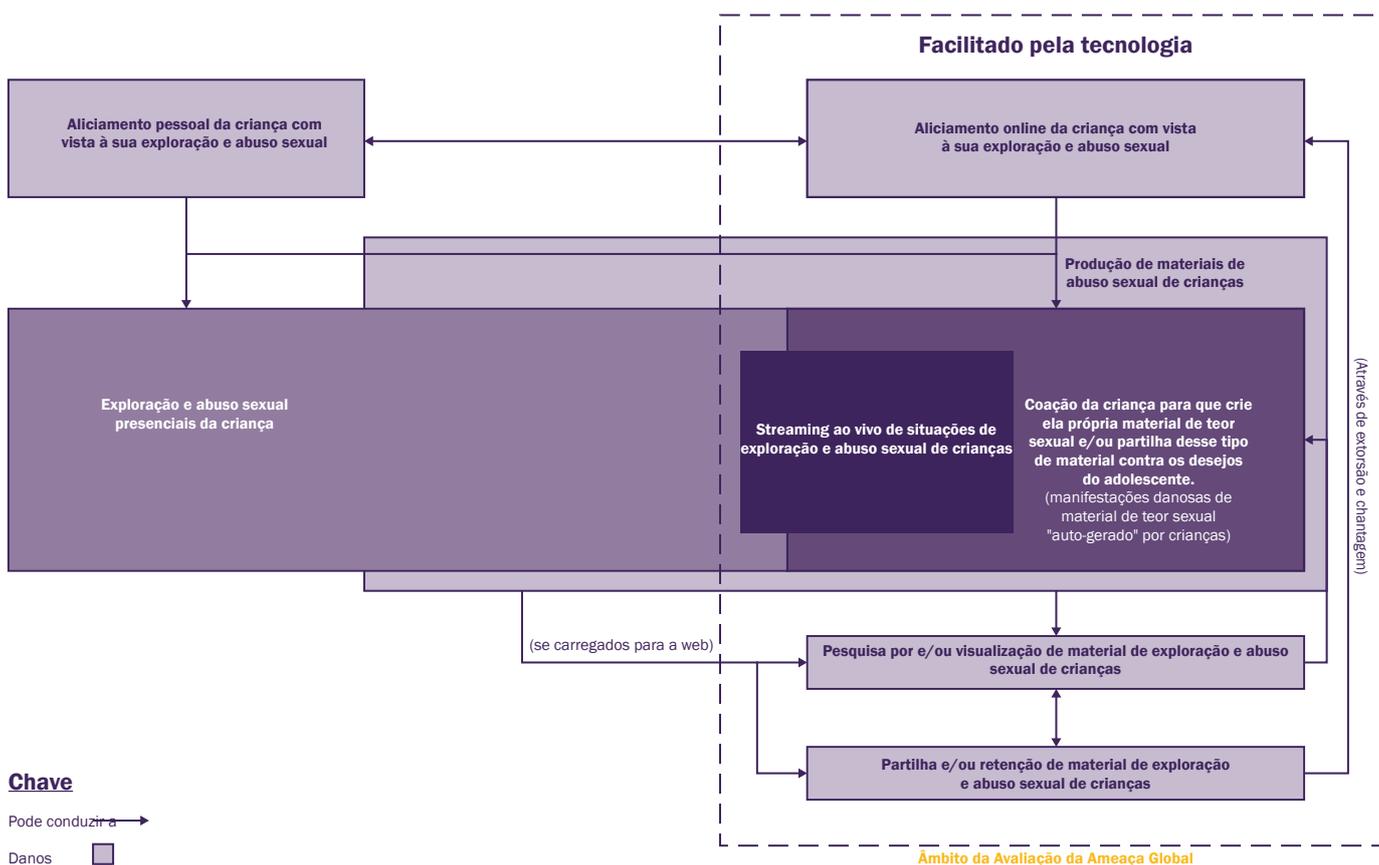
- Entrevistas com agentes das forças de segurança, defensores da segurança infantil, académicos, representantes do setor das tecnologias e vários outros especialistas.
- Estudos de caso fornecidos por organizações-membro e suas afiliadas.
- Uma pesquisa anonimizada de 32 empresas globais de tecnologia, conduzida pela Alliance em colaboração com a Technology Coalition.
- Vinhetas desenvolvidas pela Crisp, empresa líder no fornecimento de tecnologias de segurança online. Essas vinhetas estão incluídas em chamadas de texto explicativo (ver exemplo na Figura 6).

O desenvolvimento deste relatório foi orientado por um Comité Orientador composto por 20 especialistas das forças de segurança, do governo, do setor tecnológico, das Organizações Não Governamentais e Intergovernamentais (ONGs e IGOs) e universidades (ver página 66).

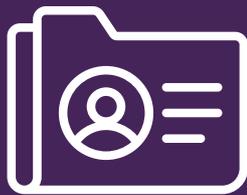
CRISP

A Crisp fornece o serviço de Actor Risk Intelligence (investigação de agentes de risco) sobre as agendas e o trabalho de indivíduos e grupos, a fim de prevenir danos online, desinformação e ataques. Através da ferramenta Actor Intelligence Graph analisa conversas digitais em tempo real para revelar as relações entre os agentes e os seus grupos, a fim de prever, tão cedo quanto possível, quaisquer danos online. O Crisp protege mais de dois mil milhões de utilizadores diariamente, abrangendo cerca de 450 milhões de crianças. www.crispthinking.com

Figura 4: Mapa dos Danos.



Abordagem da Investigação.



58

Estudos de caso revistos



+230

Artigos de literatura revistos



55

Organizações consultadas



34

Entrevistas realizadas

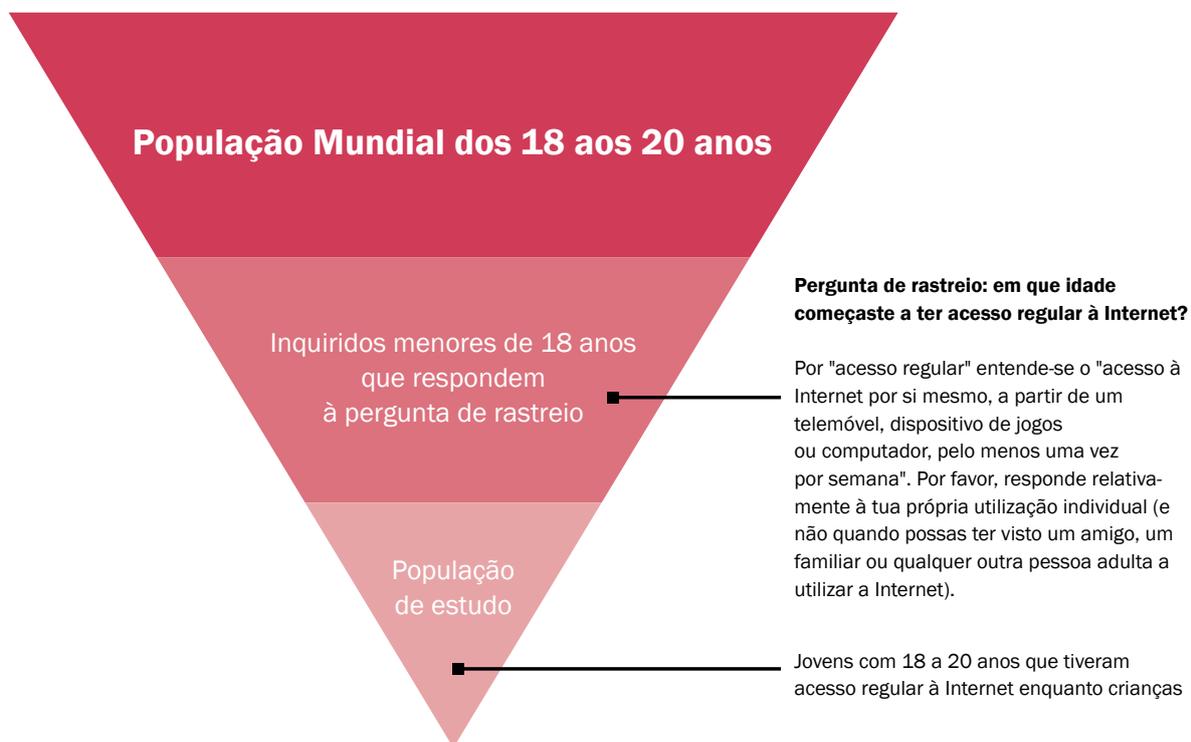
IMPACTO ECONOMISTA

Estimativas da exposição de crianças a danos sexuais online e respetivos fatores de risco.

UM ESTUDO GLOBAL SOBRE AS EXPERIÊNCIAS DE INFÂNCIA DE JOVENS DOS 18 AOS 20 ANOS

A Internet, as redes sociais e outras aplicações/plataformas digitais podem revelar-se uma faca de dois gumes para crianças e jovens. Ainda que estes ambientes forneçam fóruns importantes para a aprendizagem e interação, bem como uma plataforma para a descoberta positiva da sexualidade e a promoção das relações humanas entre as criançasⁱ, podem, ao mesmo tempo, ser usados para facilitar a exploração e o abuso sexual das crianças por adultos — conhecidos e desconhecidos —, bem como pelos seus pares, e permitir o acesso a conteúdo impróprio para estas idades.

Para ajudar a preencher a lacuna no conhecimento global sobre a potencial escala e âmbito dos danos sexuais perpetrados contra crianças online, a Economist Impact e a WeProtect Global Alliance conduziram um estudo que reúne evidências de mais de 5000 jovens entre os 18 e os 20 anos, em 54 países de todo o mundo, que tiveram acesso à Internet durante a infância.ⁱⁱ



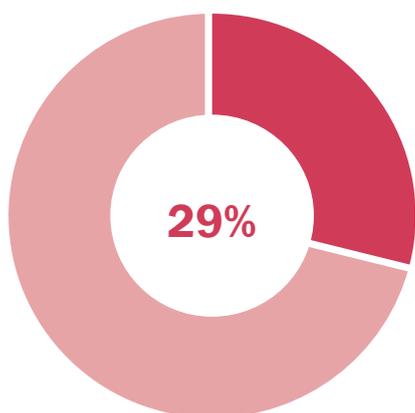
O inquérito perguntou aos entrevistados acerca da respetiva exposição a danos sexuais online e quais os fatores de risco existentes durante a sua infância. As perguntas centraram-se em quatro danos sexuais online.ⁱⁱⁱ A saber:

- Ter recebido conteúdo sexualmente explícito enviado por um adulto ou outra pessoa desconhecida, antes dos 18 anos.
- Ter-lhe sido pedido que mantivesse em segredo parte de seu relacionamento online sexualmente explícito com um adulto/ pessoa desconhecida.
- Ter tido imagens sexualmente explícitas suas partilhadas sem o seu consentimento (por um colega, adulto, ou pessoa previamente desconhecida).
- Ter-lhe sido pedido que praticasse qualquer ato sexualmente explícito online com o qual se sentia desconfortável (por um colega, adulto, ou alguém que não conhecia previamente).

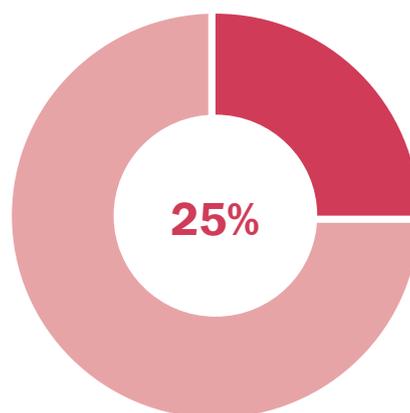
As principais conclusões desta investigação são apresentadas de seguida. As constatações integrais e a metodologia utilizada poderão ser encontradas no estudo *Estimativas de Exposição Infantil a Danos Sexuais Online e Respetivos Fatores de Risco: um estudo global acerca das experiências de infância de jovens dos 18 aos 20 anos*, no site *WeProtect Global Alliance*.

CONSTATAÇÕES-CHAVE

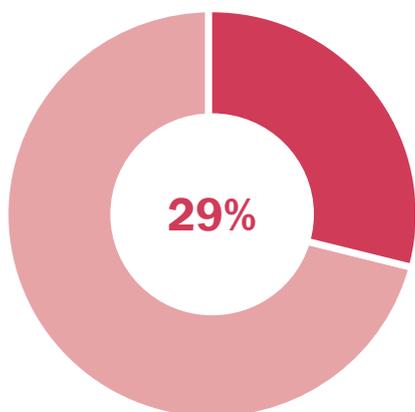
54% dos inquiridos tinham experienciado pelo menos um dano sexual online durante a infância.^{iv}



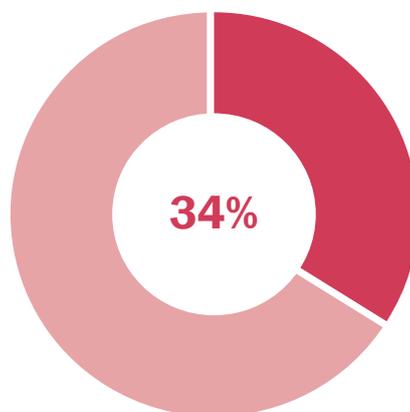
Receberam conteúdos de teor sexual explícito de um adulto seu conhecido ou de alguém desconhecido, antes de completarem 18 anos



Foi-lhes pedido, por um adulto seu conhecido ou por alguém desconhecido, que parte das suas interações online de carácter sexual explícito fossem mantidas em segredo

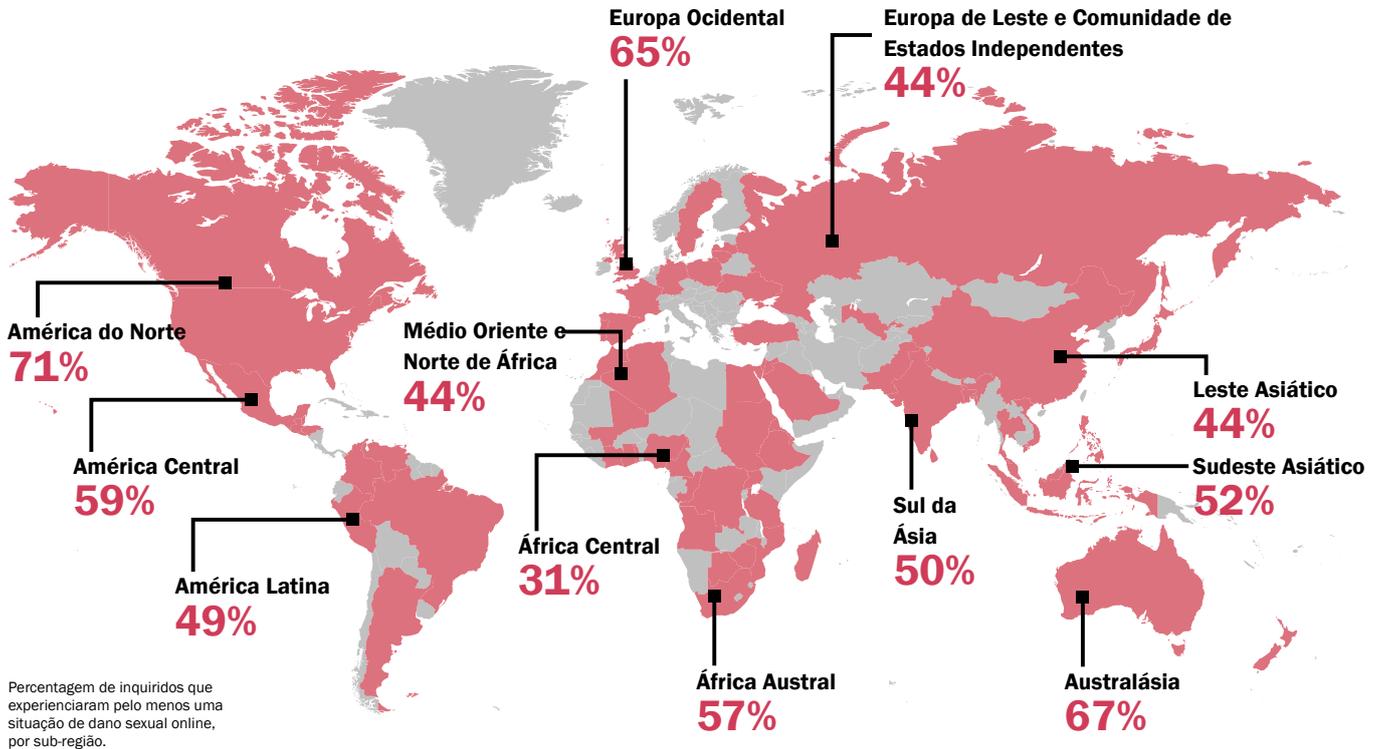


Tiveram alguém que partilhou imagens e/ou vídeos seus de carácter sexual explícito sem autorização

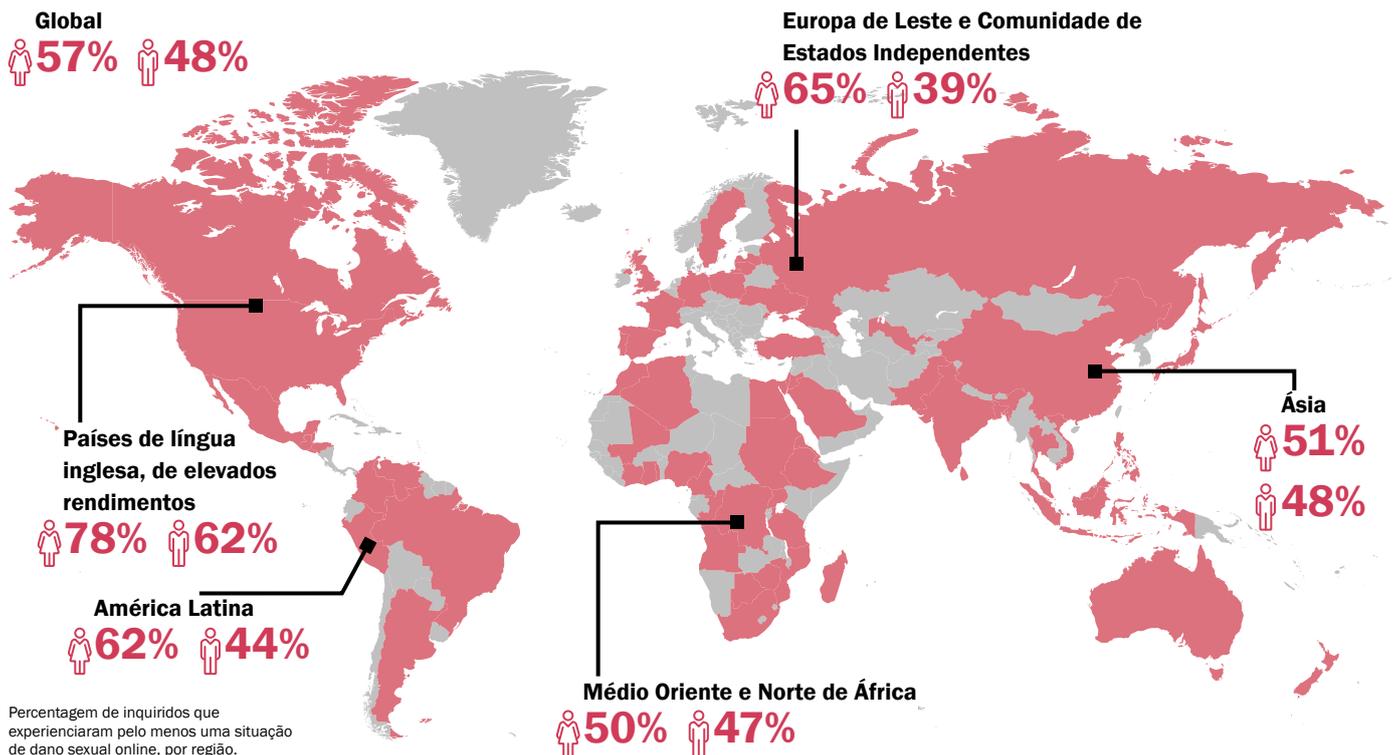


Foi-lhes pedido que fizessem algo sexualmente explícito online com o qual não se sentiam confortáveis

Os danos sexuais online em crianças **ACONTECEM EM QUALQUER LUGAR...**

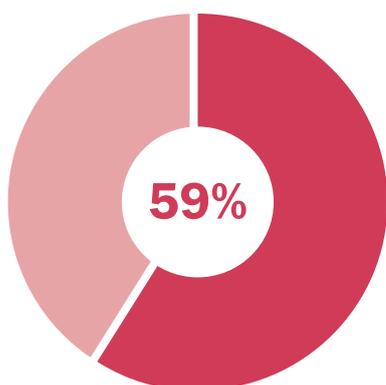


...e ainda que as raparigas corram maiores riscos, **QUASE METADE DOS RAPAZES**

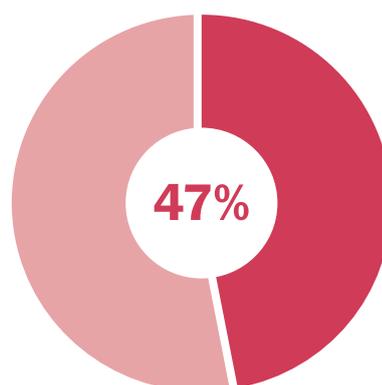


Os inquiridos que se identificavam como transgénero/não-binários, LGBTQ+ e/ou portadores de deficiência revelaram-se **MAIS SUSCETÍVEIS** de experienciar danos sexuais online durante a infância.

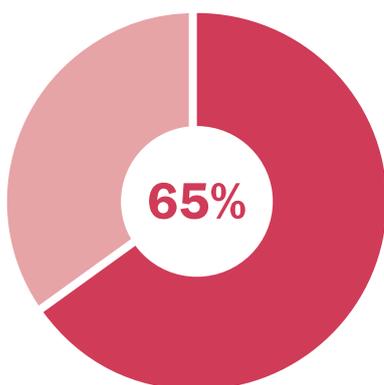
% experienciaram algum tipo de dano sexual online



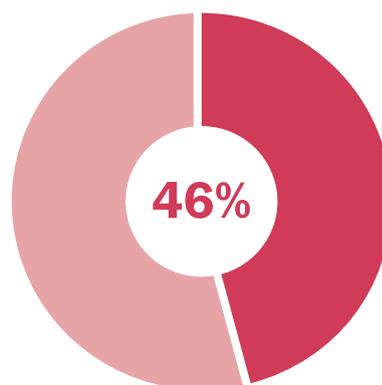
Transgénero/não-binário



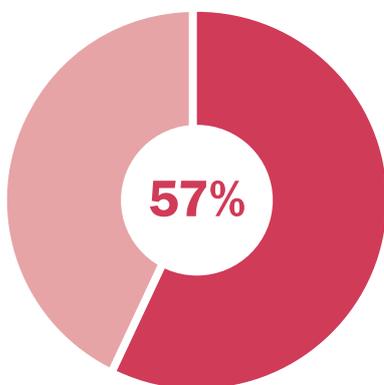
Cisgénero



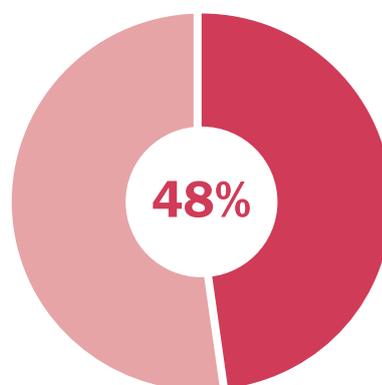
LGBTQ+



Não LGBTQ+



Deficiente

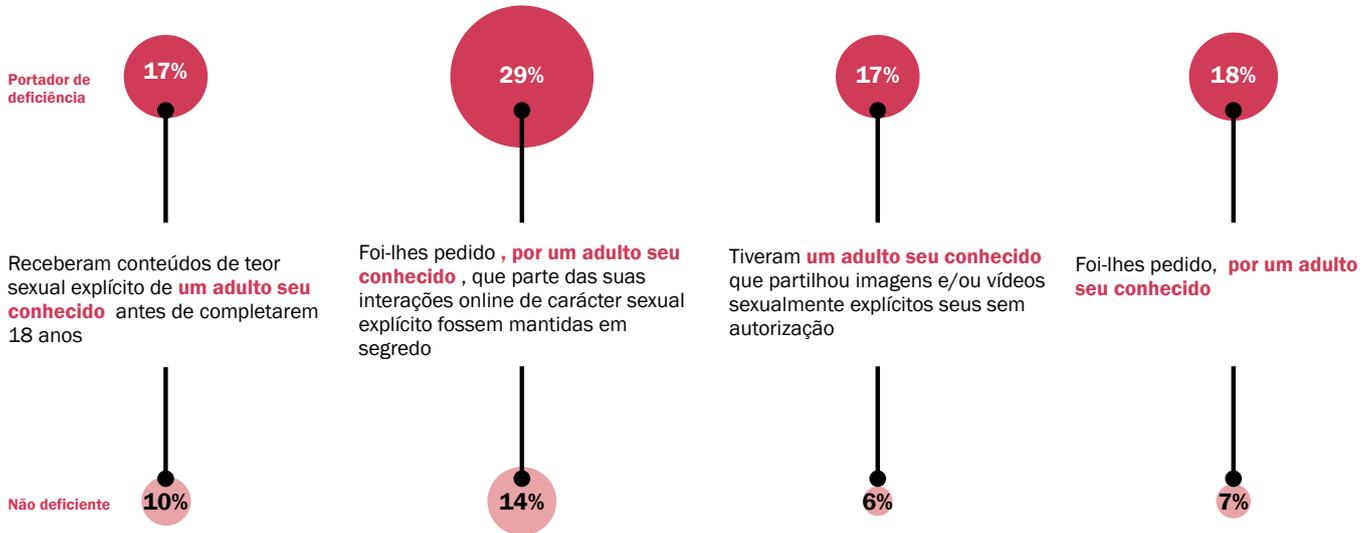


Não deficiente

Percentagem de inquiridos que experienciaram pelo menos uma situação de dano sexual online, por característica autoidentificada.

Aos inquiridos foi perguntado se se identificavam a si mesmos como transgénero/não-binário, LGBTQ+, e/ou portadores de deficiência. Os dados neste gráfico provêm de uma análise que desagregou a amostra com base nessas respostas. O número de inquiridos que se identificava com aquelas características, em qualquer uma das regiões, foi demasiado pequeno para permitir uma análise rigorosa no que diz respeito às variações geográficas das experiências para estes grupos.

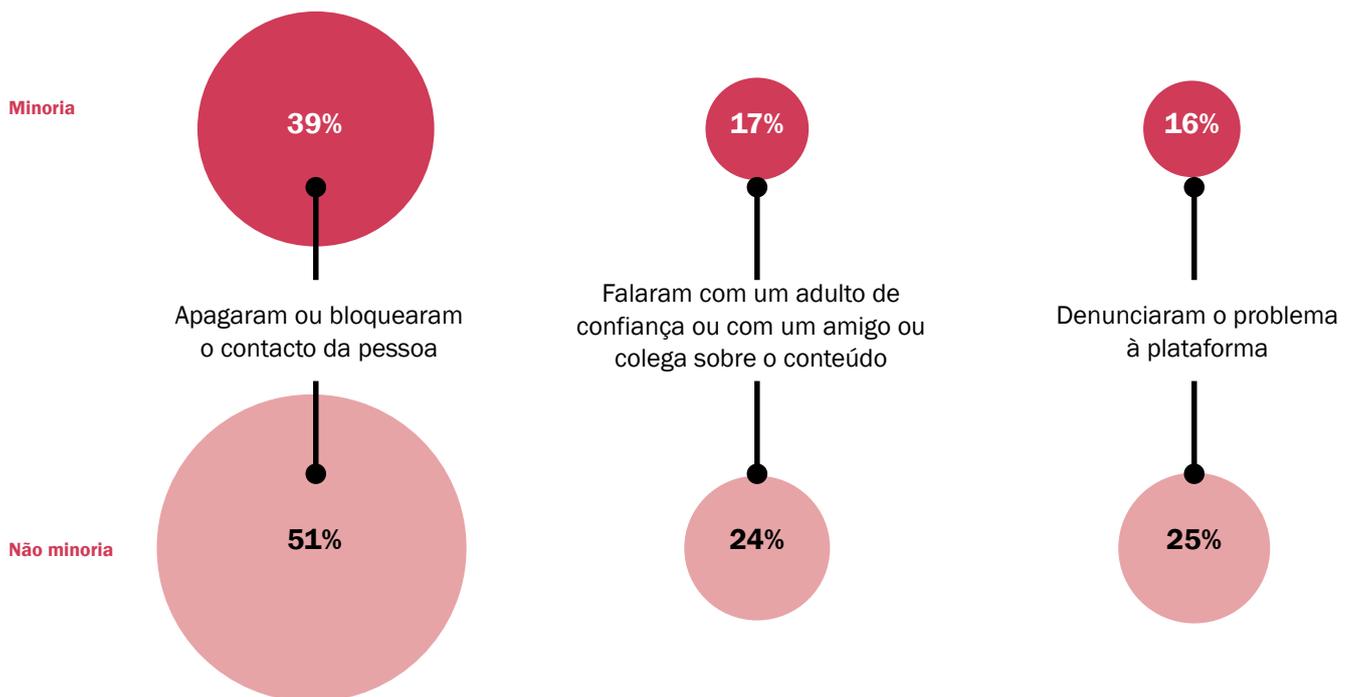
Os inquiridos que se identificavam como portadores de deficiência REVELARAM-SE mais suscetíveis de serem alvo de um adulto seu conhecido.



Percentagem de inquiridos que experienciaram danos sexuais online perpetrados por um adulto seu conhecido (deficiente ou não deficiente).

Deficiente é definido como sendo aquele que apresenta uma alteração, anomalia ou doença (física ou mental) que afete a capacidade do inquirido

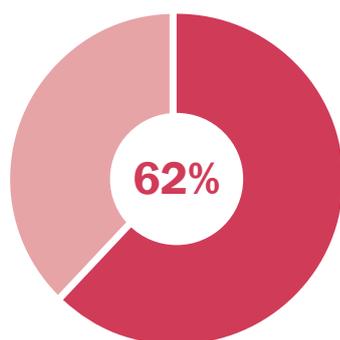
Os inquiridos que se identificavam como minorias raciais ou étnicas revelaram MENOR PROBABILIDADE de atuar nos casos em que um adulto seu conhecido ou uma pessoa desconhecida lhes tentou enviar conteúdos sexualmente explícitos.



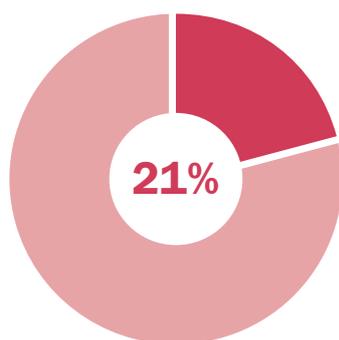
Percentagem de inquiridos que tomaram uma determinada ação (minorias e não minorias). "Minorias" é entendida como relativa a uma raça, nacionalidade ou etnia que seja diferente da maioria da população residente no país do inquirido.

DOIS TERÇOS dos inquiridos que receberam material sexualmente explícito online durante a infância, receberam-no através de um serviço de mensagens privadas, e mais frequentemente nos próprios dispositivos móveis.

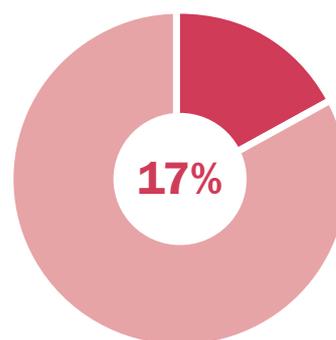
Dispositivo no qual o inquirido recebia os conteúdos



No próprio telemóvel

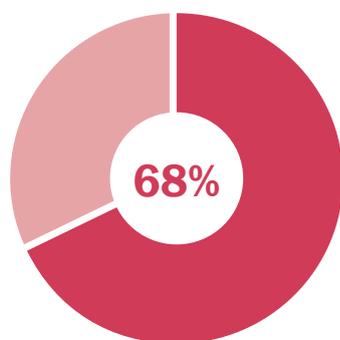


No telemóvel de um amigo

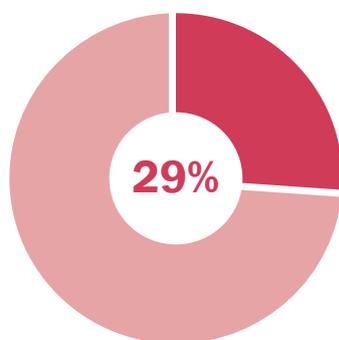


No próprio computador portátil/de secretária

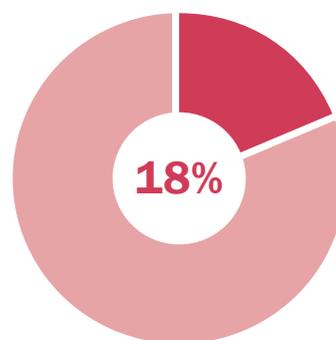
Plataforma na qual o inquirido recebia os conteúdos



Serviço de mensagens privadas



Serviço de partilha de imagens/vídeos privados



Fórum aberto nas Redes Sociais

CONCLUSÕES-CHAVE

Atualmente, a escala e a abrangência dos danos sexuais online contra crianças são provavelmente diferentes. As preocupações éticas relativamente a pesquisar crianças através de uma ferramenta baseada na Internet impediram-nos de recolher dados de inquiridos menores de 18 anos.

Por que serão os níveis provavelmente diferentes hoje em dia?

- O rápido crescimento da penetração da Internet entre indivíduos de todas as idades significa que mais crianças estão a obter acesso regular à Internet em idades mais precoces.
- Uma maior percentagem de crianças de todas as idades tem acesso mais frequente aos telemóveis de adultos e/ou de colegas, e a aceder a uma maior variedade de plataformas.
- A pandemia da COVID-19 obrigou as crianças a passarem mais tempo online, ao mesmo tempo que levou a que as pessoas em todo o mundo se sentissem mais isoladas.
- As plataformas digitais tornaram-se uma forma comum de as crianças explorarem a sua sexualidade com os colegas, sendo que esses fóruns de expressão e exploração abrem portas a novas formas de abuso e exploração.

Será necessária mais investigação para entender de que modo o cenário dinâmico da Internet e das redes sociais/plataformas digitais está a transformar a forma como as crianças interagem, e o que isso significa para sua segurança face às ameaças online. O nosso estudo é um primeiro passo para traçar um quadro global do problema e identificar que tipo de pesquisas futuras seriam de valor.

NOTAS FINAIS

- i De acordo com a respetiva definição da Convenção sobre os Direitos da Criança, "crianças" são pessoas menores de 18 anos de idade neste estudo.
- ii Por "acesso regular à Internet" entende-se o acesso independente à Internet, por iniciativa própria — ou seja, não apenas acompanhando um amigo, familiar ou outro adulto que esteja na Internet, pelo menos, uma vez por semana. Por "crianças" entende-se pessoas menores de 18 anos de idade. Para obter a discussão completa acerca de que forma este método de amostragem poderá afetar os resultados, consulte o artigo completo.
- iii Um conjunto de comportamentos danos considerados fatores de risco para a potencial ou efetiva exploração e abuso sexual de crianças.
- iv 54% dos entrevistados experienciaram um ou mais danos sexuais online mencionados neste inquérito.

METODOLOGIA

Este estudo é baseado em dados recolhidos através de uma pesquisa online com 5302 jovens entre os 18 e os 20 anos que tiveram acesso regular à Internet* durante a infância (antes dos 18 anos), e que foi conduzida entre maio e junho de 2021.

O inquérito foi realizada em 21 idiomas, em 54 países, agregados em 12 sub-regiões** — cada região contando com um mínimo de 390 inquiridos — para análise. A amostra global e a agregação regional serviram para a análise das experiências de género e outras características demográficas.

Notas:

* Por "acesso regular à Internet" entende-se ter acesso direto e pessoal à Internet (ou seja, não se trata de ver um amigo, familiar ou outro adulto aceder à Internet), pelo menos, uma vez por semana.

** Australásia, África Central, América Central, Leste Asiático, Europa Oriental e Comunidade dos Estados Independentes, Médio Oriente e Norte de África, América do Norte, Sudeste Asiático, Sul de África, América do Sul, Sul da Ásia e Europa Ocidental.

05

Temas

COVID-19

A COVID-19 criou uma "tempestade perfeita" de condições propícias ao aumento da exploração e abuso sexual de crianças, em todo o mundo.³⁰

Serão necessários vários anos até que a verdadeira dimensão do abuso decorrente da pandemia seja revelada. Até lá, os serviços da linha da frente necessitam de um reforço urgente para responder às vítimas adicionais conhecidas em resultado da COVID-19.

Embora os confinamentos possam ter propiciado a via aberta para os abusos, os impactos a longo prazo da pandemia ameaçam reforçar as motivações comerciais do abuso.

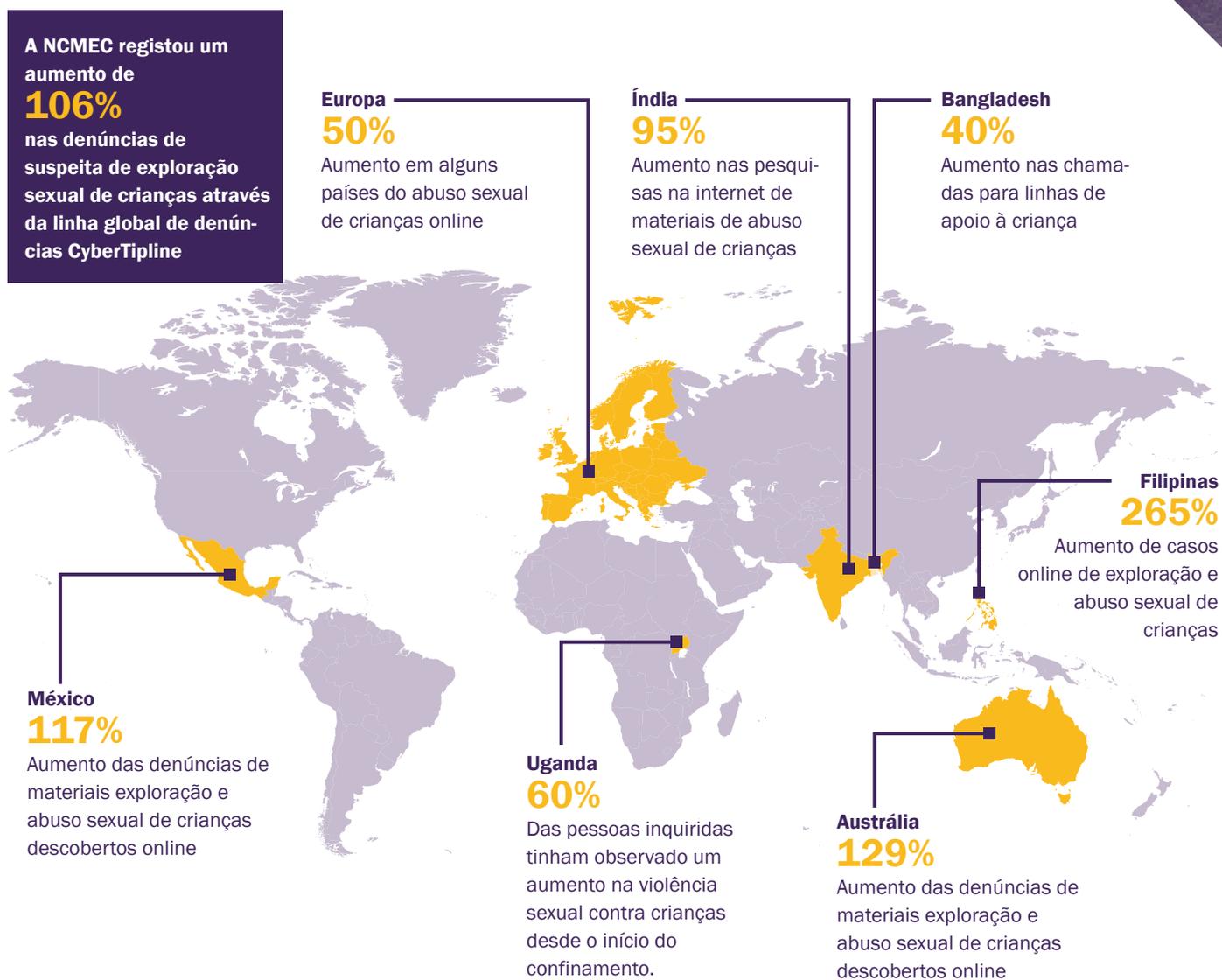
Inúmeros países relataram um aumento nos casos de exploração e abuso sexual de crianças durante a COVID-19 (ver Figura 5). A pesquisa Netclean 2020 conduzida pelas autoridades policiais em todo o mundo indicou igual consenso, transversal em toda a comunidade policial, de que se registou um aumento nas tentativas de contactar as crianças, bem como do volume de material de cariz sexual "autogerado" por crianças, para além da atividade na dark web.³¹ Algumas agências policiais preveem um aumento acrescido no volume de material de abuso sexual de crianças detetado à medida que mais moderadores retomam a sua prática profissional.³²

Lidar com este fenómeno exigirá um investimento adicional dos governos para reforçar a capacidade dos serviços da linha de frente e a colaboração das empresas tecnológicas para reduzir os atrasos na identificação e reporte dos casos.

O verdadeiro impacto da COVID-19 é difícil de identificar, principalmente porque o aumento nos relatórios de exploração e abuso sexual de crianças durante a pandemia não é necessariamente indicativo de um aumento equivalente no número de crimes. As mudanças nas práticas de trabalho, incluindo a passagem obrigatória ao teletrabalho, impactaram negativamente em algumas das principais agências no terreno. Em alguns casos, os analistas tiveram menor capacidade para avaliar relatórios ou desempenhar funções de moderação de acordo com os padrões estabelecidos, resultando num aumento de "falsos positivos".³³ Uma maior consciencialização para o problema pode estar a contribuir para o aumento sustentado observado em 2021, à medida que os meios de comunicação social e as agências policiais continuam a destacar picos alarmantes nas taxas de abusos relatados .



Figura 5: Aumento dos casos de exploração e abuso sexual de crianças durante a pandemia de COVID-19. ^{34 35 36 37 38 39 40}



Em setembro de 2020, o fecho das escolas afetou 827 milhões de alunos em todo o mundo.⁴¹

Durante a pandemia, algumas iniciativas de prevenção dirigidas aos perpetradores registraram aumento dos pedidos de serviços de auto-ajuda.^{42,43} Desde cedo, existiu a preocupação de que os indivíduos que perpetravam abusos pudessem estar em maior risco de reincidência devido a fatores como “o stress, a falta de apoio social positivo, as dificuldades em encontrar ajuda, e maiores janelas de oportunidade” em virtude dos confinamentos, sendo que todos estes fatores “estão associados ao risco de transgressão”.⁴⁴ O aumento dos pedidos de mecanismos de autoajuda sugere que tais preocupações se confirmaram, até certo ponto, e que os confinamentos podem ter propiciado e acelerado a incidência dos abusos para alguns indivíduos.

Para muitos abusadores conhecidos, os confinamentos proporcionaram mais oportunidades de contacto com as crianças (devido ao facto de estarem mais online, em casa, e na sequência do fecho das escolas) bem como uma maior autonomia para estabelecer esses contactos. Uma investigação global com pessoas que trabalhavam na linha de frente da proteção infantil, revelou que 72,8% destes funcionários afirmaram ter observado, pelo menos, algum aumento na atividade das comunidades de abuso online durante a pandemia.⁴⁵

A utilização de “serviços ocultos” (sites alojados numa rede proxy para que a sua localização não seja rastreável) aumentou igualmente, sugerindo que mais abusadores aprenderam a ocultar as suas atividades.⁴⁶ Para além disto, registou-se um aumento no abuso online por “representação” para indivíduos que, em outras circunstâncias, poderiam ter procurado abusar pessoalmente das crianças.⁴⁷ Isto é particularmente preocupante, pois algumas crianças estão agora em maior risco de abuso presencial devido a dificuldades económicas causadas ou agravadas pela COVID-19. Como destacou a ECPAT: “À medida que as famílias perdem rendimentos, especialmente no Hemisfério Sul, podem passar a encarar as “transmissões ao vivo” como oportunidades rentáveis.⁴⁸ Isto porque a pandemia aumentou a procura por transmissões ao vivo como alternativa ao abuso presencial.⁴⁹ Nesse sentido, da pandemia poderá decorrer o reforço dos vetores comerciais de abuso, a longo prazo. Existem já evidências de que as crianças estão a reagir ao enfraquecimento das perspectivas económicas, aceitando a “autogeração” de material sexual em troca de dinheiro.⁵⁰

O Banco Mundial estima que a pandemia empurrará mais 88 a 115 milhões de pessoas para a pobreza extrema, fazendo com que os números totais ascendam a 150 milhões em 2021.⁵¹

Os confinamentos aumentaram muitos dos fatores de risco de abuso. Uma intervenção oportuna para reforçar os sobrecarregados serviços da linha de frente será crítica para apoiar o acréscimo de vítimas.

Indubitavelmente, os confinamentos terão reduzido o risco de as crianças serem vítimas de abuso em ambientes fora de casa (como os ambientes institucionais). No entanto, para muitos outros, os confinamentos criaram ou agravaram as vulnerabilidades, como sejam a solidão ou as questões de saúde mental⁵²; aumentaram o tempo passado online⁵³, logo, aumentaram a exposição a predadores⁵⁴; e impediu o acesso a redes de apoio, como os adultos de confiança e os amigos que, normalmente, poderiam oferecer proteção.⁵⁵ O risco de sofrer abuso sexual online durante a pandemia terá sido maior para as crianças que experienciaram uma convergência destes vários fatores de risco.

Como salientado no Capítulo Danos: *Produção de Material de Abuso Sexual de Crianças, uma parte significativa do abuso sexual de crianças é perpetrado pela família*. Os confinamentos por COVID-19 terão feito com que muitas crianças permanecessem presas em casa junto dos seus agressores. O sofrimento dessas vítimas terá sido prolongado devido ao acesso reduzido aos canais habituais de notificação durante a pandemia. No Paraguai, as denúncias de abuso sexual de crianças diminuíram 50% durante o confinamento, apenas para aumentar após o relaxamento das medidas — presumivelmente porque as vítimas (e adultos de confiança, como professores ou profissionais de saúde) puderam sair de casa para denunciar os abusos.⁵⁶ Na Jamaica, a diminuição das denúncias oficiais de abuso foi desmentida pelo número crescente de ligações diretas, sugerindo que as crianças podem estar em situações em que as vias normais de denúncia não são acessíveis, pelo que “o abuso estará, muito provavelmente, a ocorrer no próprio lar”.⁵⁷

Na Austrália registou-se uma descida no número de denúncias de maus tratos a crianças durante a primeira fase da pandemia, apenas para se observar um disparo das queixas quando as restrições foram levantadas.⁵⁸

Em 2020, devido à pandemia, foram reportadas interrupções nos serviços de proteção à criança em 104 países, representando uma população total de 1,8 mil milhões de crianças.⁵⁹ Em muitas regiões, a capacidade de policiamento também foi afetada. De acordo com o relatório de 2020 da Netclean, a capacidade das forças de segurança para policiar e investigar a exploração e o abuso sexual de crianças caiu durante a pandemia.⁶⁰ A Interpol informou que a pandemia resultou na chegada de menos denúncias à polícia, em maiores dificuldades na progressão das investigações a decorrer, bem como na utilização reduzida da Base de Dados Internacional de Exploração Sexual Infantil.⁶¹

À medida que os países emergem dos confinamentos e as vítimas apresentam queixas atrasadas de abusos, o volume acrescido de casos resultará na acumulação exacerbada de casos pendentes nos serviços da linha de frente. Sem uma intervenção governamental atempada, o efeito dominó da COVID-19 traduzir-se-á no prolongamento do sofrimento das crianças e na redução das taxas de resolução de casos. Esta situação será tão mais provável quanto mais governos, em todo o mundo, desviarem fundos dos serviços públicos para os incentivos à recuperação económica pós-pandemia.⁶²⁶³ Tal medida enfraquecerá a resposta imediata à ameaça, podendo vir a minar a possibilidade da prevenção, de forma significativa, no futuro. Em países de baixos rendimentos, a situação pode ser agravada se outras nações seguirem o exemplo do Reino Unido na redução da Assistência Oficial ao Desenvolvimento (ODA),⁶⁴ de acordo com a alteração das prioridades de despesa. O impacto destes cortes poderá chegar ao ponto de afetar o impacto aumentado a longo prazo, de futuras crises de saúde, o que inclui a proliferação da exploração e do abuso sexual de crianças.

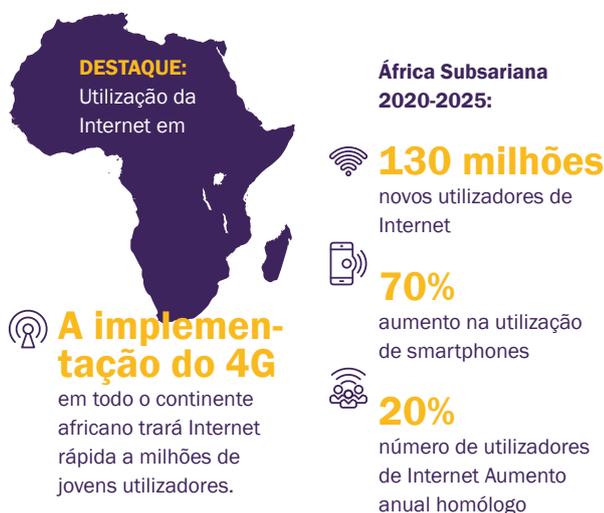
Tecnologia

O ritmo da mudança tecnológica continua a dificultar a resposta à exploração e abuso sexual de crianças online.

Contudo, nos últimos anos, as tecnologias de segurança online têm avançado significativamente. Com uma implementação mais ampla, estas ferramentas e técnicas podem facilitar a mudança de passo necessária na resposta à ameaça global.

Em 1995, menos de 1% da população mundial utilizava ativamente a Internet.⁶⁵ Hoje, essa percentagem cresceu para 59,5%.⁶⁶ As velocidades médias globais de download também estão a aumentar,⁶⁷ esperando-se que o número de dispositivos móveis ativos no mundo ascenda aos 17,62 milhares de milhões até 2024 — um aumento de 3,7 milhares de milhões de dispositivos em comparação com os dados de 2020.⁶⁸ Algumas regiões do mundo, como o continente africano (ver Figura 6), estão a adotar estas mudanças a um ritmo especialmente acelerado. Os menores de 18 anos representam 1 em cada 3 utilizadores da Internet, em todo o mundo.⁶⁹

Figura 6: Utilização da Internet em África.^{70 71 72}



Conforme salientado no Comentário Geral 25 das Nações Unidas (ver o *Glossário de Termos*), o ambiente digital facilita o acesso a uma série de direitos da criança à medida que cada vez mais funções sociais passam a integrar as tecnologias digitais. As oportunidades educacionais destas tecnologias têm potencial para serem especialmente transformadoras. O crescimento dos dispositivos móveis tem sido saudado como uma oportunidade para alcançar a população global de meninas que representam "dois terços das crianças em idade escolar fora da escola".⁷³ Para as crianças, os benefícios sociais da conectividade à Internet são igualmente amplos. De acordo com o inquérito 2020 EU Kids Online, a maioria respondeu "ser mais fácil serem eles mesmos online, pelo menos, às vezes".⁷⁴ Este fator pode ser especialmente transformador para os jovens cuja liberdade de expressão se encontra limitada de várias outras formas seja, por exemplo, por deficiências ou impedimentos, ou por habitarem um contexto socio-ambiental restritivo.⁷⁵

Para algumas crianças, os benefícios da conectividade são atualmente contrabalançados por impactos negativos e experiências de comportamentos nocivos e de abuso sexual.

Há evidências que sugerem que, para algumas crianças, estar online expõe-as a interações de cariz sexual⁷⁶ e a imagens sexuais.^{77 78} Embora algumas crianças (as mais velhas) possam perceber isso como oportunidades positivas para explorar sua identidade sexual, para outras, em particular as crianças pequenas, o impacto no desenvolvimento poderá, potencialmente, ser mais negativo.⁷⁹ Conforme explicado no capítulo Dano: Pesquisa e/ou Visualização de Material de Abuso Sexual de Crianças, a exposição habitual à pornografia está ligada ao desenvolvimento de comportamento sexual nocivo (ver *Glossário de Termos*) em adolescentes.^{80 81}

O estudo Economist Impact, realizado juntamente com este relatório, revelou que dos inquiridos que afirmaram ter recebido material sexualmente explícito, 62% receberam-no nos seus dispositivos móveis. Em muitos países, os smartphones são agora o meio preferencial de conexão das crianças à Internet.^{82 83}



A amplificação do acesso à Internet por meio de dispositivos móveis conectados contribui para a sensação de encurralamento das crianças que são vítimas de abuso, uma vez que os abusadores parecem infiltrar-se em todas as facetas do seu dia a dia.⁸⁴ O inquérito Thorn de 2021, que incidiu sobre os jovens nos Estados Unidos da América, revelou que muitas crianças respondem a interações sexuais danosas online desvalorizando o impacto destas e ocultando-as — estas táticas podem multiplicar e/ou agravar os danos causados.⁸⁵

Existem sinais positivos de que os defensores — incluindo as próprias crianças e jovens — começam a desafiar a aparente "normalização" do abuso sexual. No Reino Unido, no início de 2021, a exposição da "cultura da violação sexual" nas escolas inspirou os adolescentes a partilharem as suas experiências de assédio sexual como parte do movimento "Everyone's Invited" (Estão Todos Convidados). Desde então, este movimento reuniu mais de 50.000 depoimentos, gerando um movimento semelhante nos EUA.^{86 87 88} Ainda que a Internet tenha desempenhado um papel na proliferação da exploração e do abuso sexual, por outro lado, proporciona aos jovens uma plataforma a partir da qual podem expressar-se e exigir mudanças.⁸⁹

Muitas das forças policiais não dispõem dos recursos necessários para investigar a exploração e o abuso sexual de crianças online.

Até mesmo os criminosos com escassos conhecimentos técnicos conseguem dificultar a deteção de crimes informáticos recorrendo a soluções de anonimato como o Tor e as Redes Privadas Virtuais (VPNs), agora tão comuns e já integradas de origem em alguns navegadores de Internet.⁹⁰ O uso de encriptação também tem vindo a aumentar (ver Capítulo Danos: *Regulação, Cooperação Voluntária e Transparência*). O efeito geral é uma obstaculização significativa das investigações policiais, causadas por tecnologias de fácil acesso. Na Dark Web, os abusadores representam um desafio num patamar inteiramente diferente. Entre os tecnologicamente mais avançados, os abusadores exploram as oportunidades oferecidas pelas novas ferramentas para facilitar a sua ação criminosa e evadir a deteção.

Estima-se que o número de dispositivos móveis ativos em todo o mundo deverá alcançar os

17,62 MIL MILHÕES

até 2024

O estudo Economist Impact, realizado em conjunto com este relatório, revelou que, dos inquiridos que afirmaram ter recebido material sexualmente explícito

62%

receberam-no nos seus dispositivos móveis.

Os abusadores usam a dark web para procurar novas ferramentas que suportem a sua ação criminosa.



Os abusadores na dark web estão cada vez mais sofisticados e confortáveis com as tecnologias de ponta usadas para criar e distribuir material de abuso sexual de crianças. Para tornar tudo ainda mais complicado, existe toda uma geração emergente de abusadores na dark web com conhecimentos de tecnologia que empregam e promovem métodos e serviços de segurança avançados para evadir a detecção.

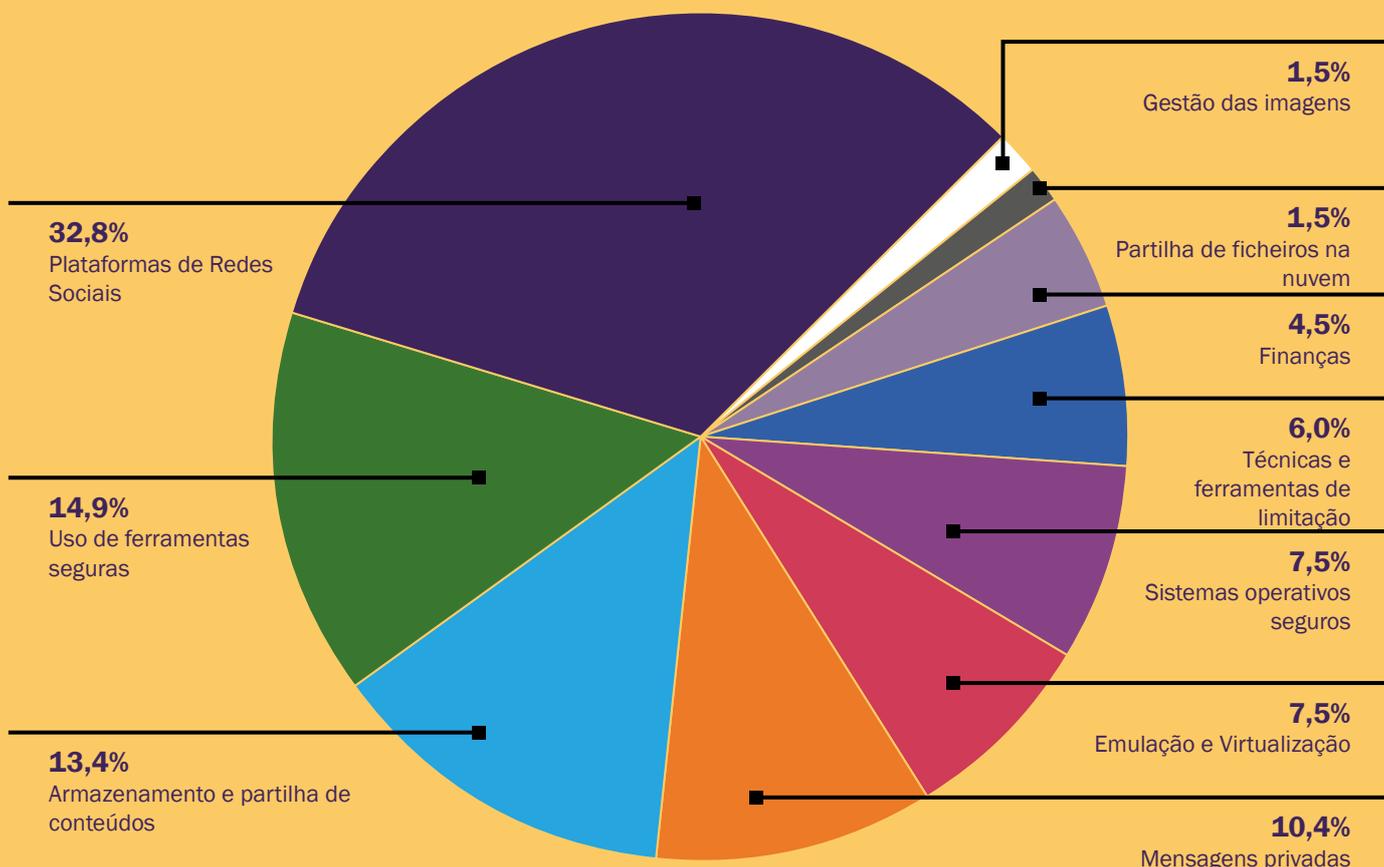
Tornando cada vez mais difícil a investigação policial assim como os processos criminais, esses infratores procuram continuamente novas alternativas e soluções para facilitar a exploração de crianças online. De forma preocupante, o kit de ferramentas operacionais destes criminosos vem evoluindo e crescendo na mesma proporção daquilo que é feito em termos de inovação das tecnologias digitais.

Os analistas do Crisp avaliaram o nível de interesse do perpetrador pelos tópicos de tecnologia ao examinar de perto as conversas que ocorreram em variados fóruns de criminosos na dark web, em fevereiro de 2021.

Dos vários "tópicos de tecnologia" discutidos nesses fóruns, quase um terço estava relacionado com plataformas nas quais os infratores pretendiam aliciar crianças ou utilizadores vulneráveis, para além das discussões mais amplas sobre "tradecraft" (ver o *Glossário de Termos*). Foi detetado ainda que mais de dois terços das discussões se centravam em tópicos como ferramentas técnicas para mensagens diretas, trocas monetárias ou como adquirir e armazenar conteúdos em segurança, tanto localmente como na nuvem — todos eles podendo tornar mais difícil a identificação e condenação dos criminosos.

Para conhecer as definições dos tópicos de tecnologia, consulte o *Glossário de Termos*.

Figura 7: Tópicos de tecnologia discutidos nos fóruns de criminosos da dark web.



Tal como em outros crimes facilitados pela Internet, a exploração sexual de crianças e o abuso online apresentam, para muitas agências policiais, desafios fundamentais à investigação: mais recorrentemente, as capacidades digitais limitadas, a baixa qualificação dos funcionários, a falta de acesso a ferramentas que agilizem o processo de investigação. O Sri Lanka reportou recentemente a falta de técnicos nas unidades de investigação,⁹¹ já a polícia tailandesa afirmou que precisa de mais recursos treinados na investigação de pagamentos da dark web e criptomoeda associados às práticas de abuso online.⁹²

Alguns países gerem estas dificuldades optando por agregar os crimes de exploração e abuso sexual de crianças online ao conjunto de unidades de crimes cibernéticos, onde os casos acabam por competir pela atenção e disponibilidade dos agentes, devido ao elevado volume de trabalho, e também face à elevada complexidades de alguns desses crimes, nomeadamente a fraude. Em alguns locais, a cooperação com prestadores de serviços online também fica para trás. De acordo com a Interpol, o incumprimento de mandados policiais é um grande desafio global.⁹³ As discrepâncias nas políticas corporativas relativamente à retenção dos dados resultam numa maior dificuldade da recolha de provas e evidências para as agências policiais. A raiz de muitos destes problemas é o subfinanciamento crónico das atividades policiais.

É urgente o reforço do financiamento no sentido de construir novas competências de investigação digital para as Polícias em todo o mundo, desenvolvendo e melhorando os mecanismos de colaboração transnacionais essenciais para enfrentar com eficácia esta criminalidade tecnologicamente sofisticada.⁹⁴

Alguns dos quadros legais dos diferentes países não estão ainda ajustados à era digital, criando lacunas passíveis de gerar um sentimento de impunidade relativamente abuso sexual de crianças online.

Nas últimas décadas, tem sido observada maior consistência nas abordagens legislativas ao abuso sexual infantil, catalisadas por instrumentos legais internacionais como a Convenção de Lanzarote (ver *Glossário de Termos*). Contudo, as lacunas persistem. Desde 2006, o Centro Internacional para Crianças Desaparecidas e Exploradas vem conduzindo regularmente revisões da legislação sobre os materiais de abuso sexual infantil nos 196 países membros da Interpol. O primeiro inquérito permitiu concluir que, em apenas 27 dos países inquiridos, legislação é considerada "suficiente". Na última edição (de 2018) revela que 71 países precisam ainda de definir o que constitui "material de abuso sexual de crianças", enquanto que apenas 32 exigem que os fornecedores de serviços de Internet denunciem este tipo de crime.⁹⁵

O papel da tecnologia na exploração sexual infantil e crimes de abuso levanta uma série de desafios legislativos específicos.

As discrepâncias no tratamento do abuso online "versus o abuso presencial são comuns, sendo citadas como a razão pela qual os criminosos da Internet, aparentemente, continuam a operar com impunidade. Uma análise de caso pela instituição de solidariedade International Justice Mission (IJM) destacou que apenas a Escócia, o Canadá, a Austrália e a Suécia punem a transmissão ao vivo de abuso "em igualdade de condições com o crime por contacto".⁹⁶ Muitos países também não têm uma posição legal definida sobre o uso de material fotográfico de abuso sexual infantil.^{97 98} O impacto dessa lacuna pode crescer à medida que os abusadores diversificam os métodos de produção, recorrendo a tecnologias como imagens geradas por computador (CGI) (ver o capítulo Dano: *Produção de Material de Abuso Sexual de Crianças*). Essas falências suscitam um sentimento de impunidade que alimenta a criminalidade, até porque foi observado que os abusadores visam, propositadamente, crianças em jurisdições com disposições legais deficientes.⁹⁹

A boa notícia é que já existe tecnologia capaz de proteger as crianças e capturar os abusadores, e que, com ampla adoção das ferramentas e técnicas de segurança online, estas poderão transformar a resposta global às ameaças.

Nos últimos anos, foram registados avanços significativos no que diz respeito às tecnologias da segurança online. Os exemplos principais são, entre outros:

- Ferramentas de deteção de aliciamento e preparação e funcionalidades de "Safety by Design" que reduzem a oportunidade do abusador e promovem comportamentos seguros online (ver o capítulo Danos: *Aliciamento online de crianças para fins de abuso e exploração sexual*).
- Mecanismos de dissuasão que cortam o acesso à prática do crime (ver o capítulo Danos: *Pesquisa por e/ou visualização de material de exploração e abuso sexual de crianças*).
- Hash-matching (ver o *Glossário de Termos*) soluções para detetar e remover material "conhecido" de abuso sexual infantil, e classificadores utilizados para detetar material de primeira geração (ver o capítulo Danos: *Partilha e/ou retenção de material de abuso sexual de crianças*).

O setor das tecnologias de segurança, em plena expansão, tem vindo a desempenhar um papel fundamental no desenvolvimento de muitas dessas tecnologias. Somente no Reino Unido, onde as empresas de tecnologias de segurança detêm, coletivamente, uma participação de 25% do mercado global, o setor registou uma taxa de crescimento anual estimada de 35% desde 2016,¹⁰⁰ indo a caminho de atingir £1 milhar de milhões em receitas até 2024 (ver Figura 8 abaixo).¹⁰¹ Mais de metade (52%) das empresas do Reino Unido têm uma presença internacional estabelecida.¹⁰²

Ao reduzir as oportunidades dos abusadores e aumentar a proteção oferecida às crianças, as tecnologias de segurança online podem, potencialmente, impulsionar a resposta global à exploração e ao abuso sexual de crianças online. Isto sem levar em consideração o possível impacto das ferramentas e técnicas em fase em desenvolvimento, como sejam:

- Reconhecimento facial melhorado, o que poderá acelerar a identificação de crianças vitimizadas.¹⁰³
- A análise preditiva, que já é usada por algumas autoridades para identificar crianças em alto risco de abuso, e para permitir a intervenção precoce.¹⁰⁴
- Ferramentas que podem recolher metadados (ver o *Glossário de Termos*) para detetar material de potencial abuso sexual de crianças, mesmo que o material em si não seja detetável.¹⁰⁵
- Técnicas de "impressão digital" da câmara que permitem atribuir fotografias e/ou vídeos a um dispositivo específico. Em alguns países, estas técnicas já estão a ser empregues para agilizar e fortalecer os processos judiciais.¹⁰⁷

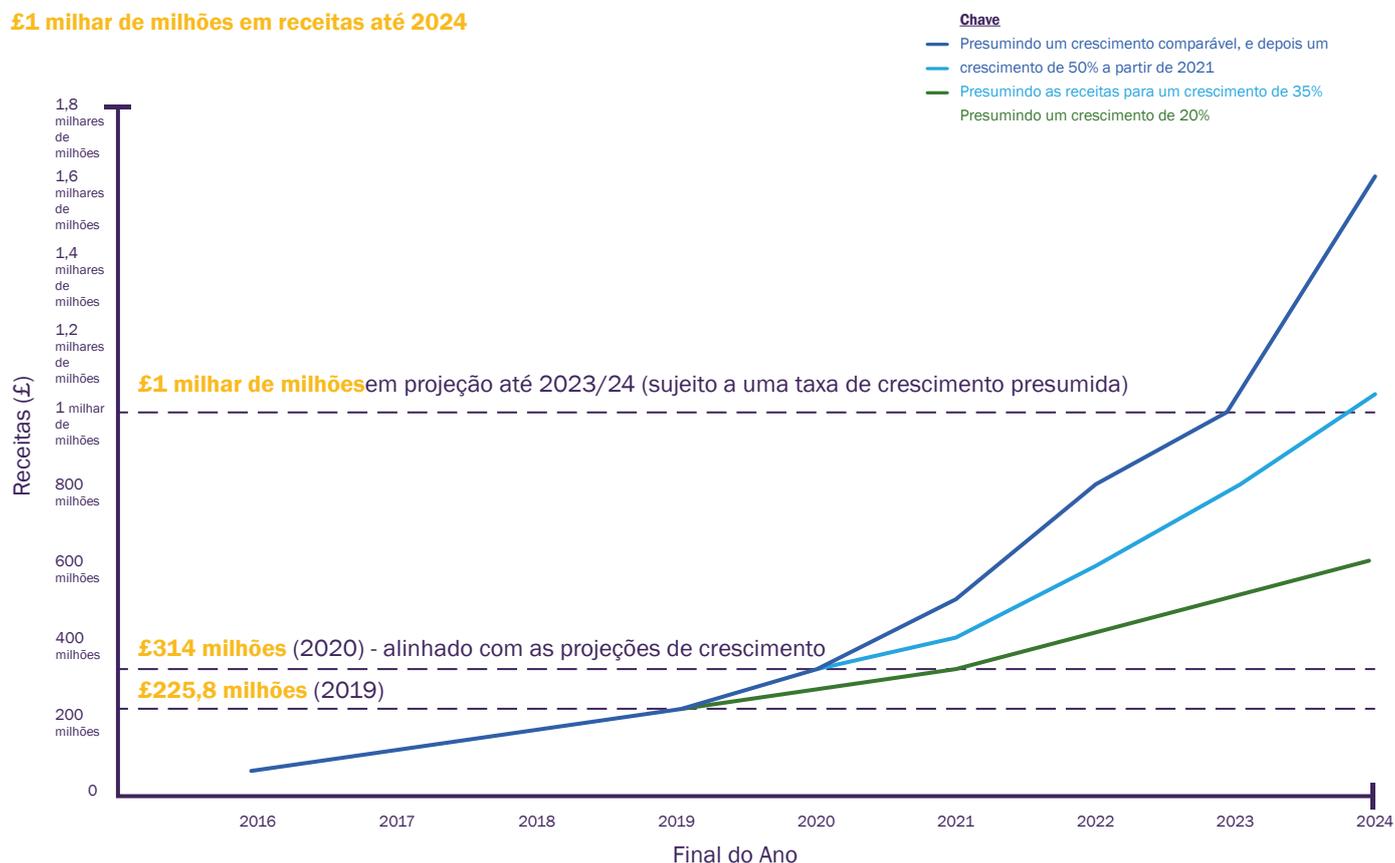
O QUE É A "SAFETY TECH"?



Os fornecedores de Safety Tech (tecnologia de segurança) desenvolvem tecnologia ou soluções tecnológicas que facilitam uma experiência online mais segura, e protegem os utilizadores de conteúdos, contactos ou condutas danosas.¹⁰⁶

Figura 8: Gráfico ilustrativo da projeção de crescimento da indústria de tecnologia de segurança no Reino Unido, reproduzido com autorização do UK Department for Digital, Media, Culture, and Sport.¹⁰⁸

£1 milhar de milhões em receitas até 2024



APPLE: PROTEÇÕES ALARGADAS PARA CRIANÇAS

A Apple está a ponderar a introdução de funcionalidades adicionais de segurança infantil nos Estados Unidos.

A saber:

- Novas ferramentas, ao nível do dispositivo, que alertariam as crianças e, no caso de menores de 13 anos, os seus pais ou responsáveis, sempre que forem recebidas ou enviadas fotos sexualmente explícitas, caso os pais ou responsáveis optem por ativar essa notificação.
- Atualizações à Siri e à Pesquisa para assistir os utilizadores na eventualidade de se depararem com situações sexualmente inseguras, online e offline, e também para intervir quando os utilizadores tentarem pesquisar material de abuso sexual infantil, indicando recursos e disparando avisos vocacionados para prevenção do abuso.
- Aplicação da nova ferramenta NeuralHash para identificar material "conhecido" de abuso sexual de crianças, que esteja armazenado na biblioteca de fotos do iCloud, "comparando e procurando a correspondência" do conteúdo com um banco de dados hash de imagens de abuso sexual de crianças. Se a correspondência de hashes exceder um limiar mínimo, é acionada uma verificação humana para confirmação prévia a um relatório a ser enviado ao NCMEC. O processo de correspondência é alimentado por uma tecnologia criptográfica chamada Private Set Intersection and Threshold Secret Sharing, que determina se existe uma correspondência sem revelar o resultado — a menos que e até que o limiar seja atingido. A Apple não pode reter quaisquer dados sobre a conta de um utilizador, exceto se uma coleção de imagens correspondentes ao CSAM "conhecido" tiver sido detetada.

No limite, os recursos podem ser compatíveis com o serviço de mensagens encriptadas da Apple, o iMessaging, demonstrando o seu potencial continuado para contrariar as ameaças de exploração e abuso sexual de crianças, até mesmo em ambientes encriptados, pela adoção de tecnologias ao nível do dispositivo bem como do lado do servidor, e preservando a privacidade dos dados.

GLOBAL PARTNERSHIP TO END VIOLENCE AGAINST CHILDREN: SAFE ONLINE FUND

A iniciativa Safe Online faz parte da Global Partnership to End Violence Against Children (Parceria Global pelo Fim da Violência Contra as Crianças). Trata-se de um fundo que investe em intervenções programáticas, produção de prova e inovação tecnológica para o combate ao abuso sexual de crianças online. Desde 2017, a Safe Online já investiu um total de 48 milhões de dólares em 60 projetos. Em 2020, investiu 10 milhões de dólares na conceção e integração de soluções de tecnologia.

Em conjunto com os investimentos financeiros para reforço da resposta ao abuso sexual de crianças online, a iniciativa Safe Online, da End Violence Partnership, promove a produção de conhecimento e a colaboração para maximizar a utilização de recursos coletivos e garantir que os investimentos tenham um impacto mais amplo.

OSafe Online desempenha um papel fundamental na defesa e condução de ações colaborativas para alinhar os esforços globais, regionais e nacionais para combater os danos online contra crianças.

Esta visão está dependente de os governos e as empresas do setor privado aumentarem o investimento no desenvolvimento das soluções de segurança para as crianças. Tal como foi salientado pela End Violence Partnership, a falta de investimento mantém-se como o maior obstáculo a uma resposta eficaz à exploração sexual de crianças e ao abuso online.¹⁰⁹Uma adoção abrangente e consistente destas tecnologias será a chave para evitar que os abusadores simplesmente desviem as crianças para plataformas onde não existem mecanismos de segurança integrados.

À medida que a adoção das ferramentas se expande, o alinhamento internacional sobre a base legal para o uso de tais tecnologias tonar-se-á cada vez mais determinante,¹¹⁰ reconhecendo que muitos levantam considerações éticas e de privacidade. Os governos precisam conferenciar com profundidade com as empresas a fim de prosseguir o desenvolvimento de quadros legais que permitam uma inovação responsável que coloque os direitos das crianças no centro da concepção e da implantação das tecnologias. Este processo deverá contar também com a proteção do direito das crianças à privacidade, com explicações "adequadas à idade" e a não discriminação na aplicação de algoritmos de IA.¹¹¹Os mecanismos de proteção das crianças mais jovens merecem uma especial consideração para que se assegure que aquelas não sejam privadas de oportunidades devido aos riscos percebidos, nem mesmo porque o baixo nível de alfabetização digital pode, em última análise, torná-las mais suscetíveis a abusos.¹¹²

Regulação, cooperação voluntária e transparência

O ritmo da mudança tecnológica continua a dificultar a resposta à exploração e abuso sexual de crianças online.

Nos últimos anos, a proliferação da exploração e do abuso sexual de crianças online vem alimentando o debate sobre a regulamentação da Internet.

À medida que mais países avançam para regulamentar os prestadores de serviços online, a cooperação voluntária e a transparência continuam a ser determinantes para uma resposta global coerente e coesa.

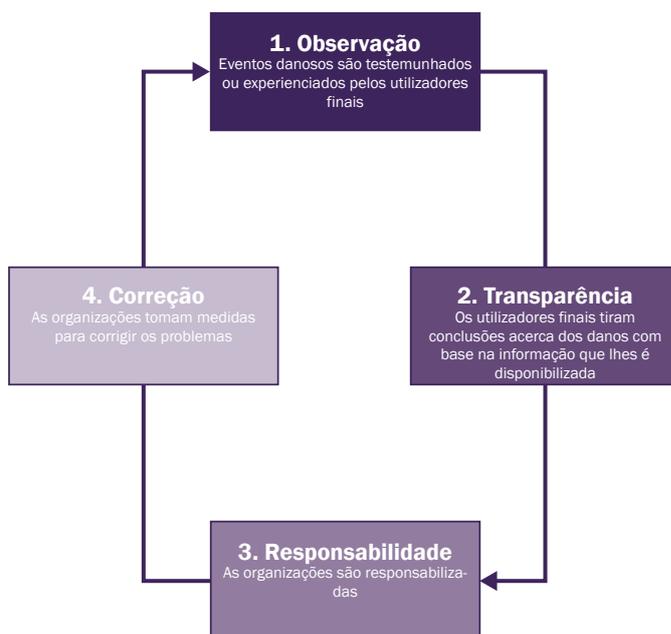
A regulamentação visa disponibilizar regras-padrão que permitam contrabalançar a privacidade com a segurança do utilizador, favorecendo uma abordagem mais consistente na abordagem aos danos online.

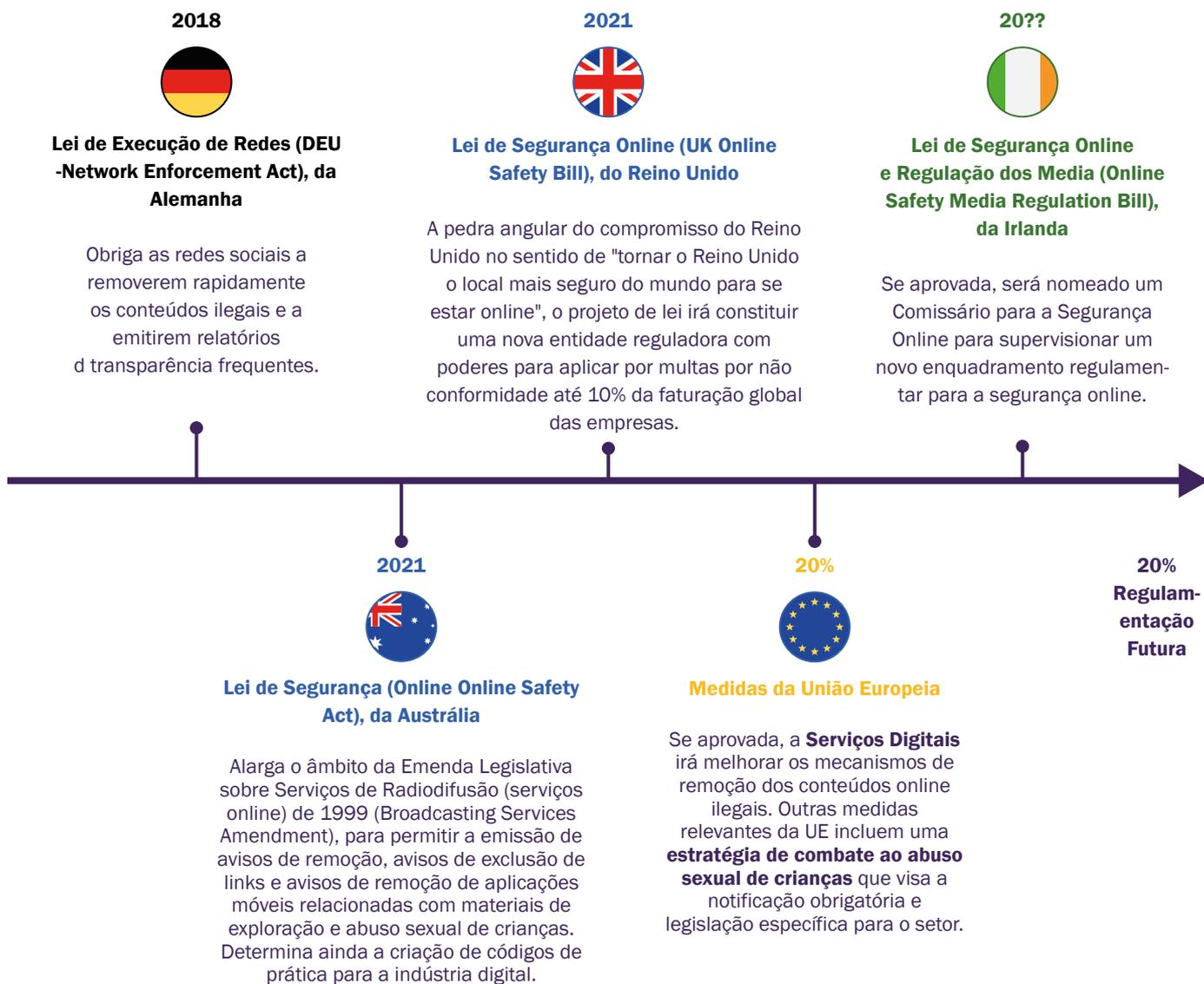
Nos três últimos anos, notou-se um avanço significativo na direção da regulamentação dos serviços digitais e da segurança online. Entre os primeiros a procurar uma solução legislativa estão a Austrália, a Alemanha, o Reino Unido, a União Europeia e a Irlanda (ver a Figura 10).

Os sistemas regulatórios eficazes seguem um ciclo consistente de quatro etapas (ver a Figura 9).

A regulamentação sobre danos online é relativamente imatura em comparação à de outros setores — como a aviação, a indústria alimentar e os serviços financeiros. A transparência é limitada, sendo que a responsabilidade voluntária e as ações corretivas são inconsistentes. No entanto, o aumento da consciencialização sobre os danos está a criar uma crescente pressão internacional que clama por uma transparência consistente, critérios de responsabilidade e ações corretivas a serem aplicadas por meio de legislação e regulamentação.

Figura 9: Passos de um sistema regulatório eficiente.





No mundo físico, os quadros legais ajudam as empresas e as autoridades a equilibrar os direitos da privacidade e da segurança individuais, mas no plano online, os critérios são ainda incipientes. Ao clarificar as responsabilidades dos prestadores de serviços online, a regulamentação estabelecerá um equilíbrio mais consistente para assim melhor proteger os utilizadores da Internet contra os danos, muito especialmente, as crianças.¹¹⁹

A utilização crescente da End-to-End Encryption (E2EE) ilustra bem o risco de não dispor de critérios de segurança online consistentes, reforçando a tese da necessidade de regulação.

A encriptação e a E2EE vêm crescendo em popularidade nos anos mais recentes, à medida que o público se torna mais consciente quanto à proteção dos seus dados online, assim como da sua privacidade. A E2EE é uma das formas de proteção da privacidade mais eficazes que existem. O Relator Especial da ONU para a Liberdade de Expressão descreveu o E2EE como sendo "o bloco de construção mais básico para a segurança digital nas aplicações de mensagens instantâneas", salientando a proteção que pode oferecer às minorias em "sério risco de perseguição e violação dos direitos humanos".¹²⁰ A E2EE já vem integrada em alguns serviços de mensagens instantâneas, sendo que um conjunto de importantes plataformas anunciou já planos para implementar¹²¹ ou estender a funcionalidade.¹²²

O QUE É A ENCRIPTAÇÃO "END-TO-END" (E2EE)?

Uma forma de encriptação em que o conteúdo de cada mensagem é visível apenas para o remetente e para o destinatário. A descodificação da mensagem requer uma chave de desencriptação privada trocada apenas entre os correspondentes, de modo a que, ainda que a mensagem possa ser interceptada, ela não pode ser visualizada nem monitorizada pelo prestador do serviço, pelas autoridades policiais ou por terceiros.¹²³

Por outro lado, a E2EE acaba por minar os esforços para combater a exploração sexual infantil e o abuso online. A maioria das tecnologias de deteção, como sejam a "correspondência por hash" os algoritmos de deteção de aliciamento, os classificadores de identificação de material de abuso sexual de crianças, não são prontamente implementáveis em ambientes E2EE.

O desacordo na Europa sobre o uso de tecnologias de detecção automatizada trouxe uma antevisão inadvertida das possíveis consequências de deixar de ser possível implementar essas ferramentas. O NCMEC registou uma redução de 58% nas denúncias recebidas através da Cyber Tipline na UE, aquando da descontinuação do seu uso por algumas empresas em dezembro de 2020, a fim de cumprir a diretiva europeia para a privacidade eletrónica.^{124 125} Foi acordada uma derrogação temporária à legislação, em maio de 2021,¹²⁶ o que apenas permite que a detecção seja restabelecida por três anos. Conforme destacado pela ECPAT,¹²⁷ é necessário que exista uma resposta legislativa para o longo prazo de modo a resolver esta questão. Espera-se que a adoção, pela UE, de uma nova estratégia para os direitos da criança,¹²⁸ juntamente com o trabalho desenvolvido para melhorar a luta contra o abuso sexual de crianças online,¹²⁹ venha a abrir caminho para uma solução.

Pelo facto de ocultar a dimensão da exploração sexual de crianças e abusos detetáveis online,¹³⁰ a proliferação da E2EE poderia dificultar a argumentação a favor de um maior investimento no combate à ameaça.¹³¹ Também é provável que obstaculize as investigações das autoridades policiais, já que os pedidos de mandatos para acesso aos dispositivos dos suspeitos (para proteger as provas dos crimes) não seriam capazes de citar o conteúdo das comunicações. Em vez disso, estes ficariam limitados à incorporação de metadados (ver o *Glossário de Termos*) e de outros indicadores que apontem para uma "provável" atividade suspeita.¹³² Embora este tipo de investigação secreta possa ser usada pelas plataformas para monitorizar os utilizadores de elevado risco, conforme explicado pela Virtual Global Taskforce, os metadados "são geralmente insuficientes para atingir o limiar necessário para justificar um mandado de busca e apreensão".¹³³ A National Crime Agency (NCA) do Reino Unido chamou à atenção para a sua investigação sobre o prolífico infrator online David Wilson, que usou perfis falsos nas redes sociais para enganar, pelo menos, 500 rapazes para que lhe enviassem vídeos e imagens sexuais de si mesmos e que, seguidamente, os chantageou e aterrorizou. O NCA alertou que não só a E2EE teria reduzido a probabilidade dos crimes de Wilson terem sido detetados, mas também que teria, potencialmente, impedido o acesso às 250.000 mensagens que forneciam as provas dos crimes e que serviram para o condenar.¹³³ A utilização crescente de E2EE poderá ainda prejudicar a detecção de crimes de abuso sexual em ambientes não encriptados, reduzindo o acesso a material de abuso sexual de crianças que é necessário para treinar classificadores e outras ferramentas que detetam conteúdos ilegais.¹³⁵

Está a decorrer um trabalho de inovação com o objetivo de tornar as ferramentas de detecção compatíveis com a E2EE. A encriptação "homomórfica" começa a emergir como uma solução potencial que oferece uma forma de analisar dados encriptados sem necessidade de os desencriptar previamente.¹³⁶

Os esforços da investigação estão focados em melhorar a eficiência da tecnologia de modo a permitir a sua implementação em maior escala. São exemplos de outras propostas:

- A integração de ferramentas de detecção nos navegadores de Internet e nos sistemas operativos dos dispositivos móveis, reduzindo, desse modo, a dependência das plataformas para a detecção dos abusos.¹³⁷
- O uso de 'enclaves' seguros que forneceriam um ambiente protegido para desencriptar, digitalizar e, em seguida, voltar a encriptar o conteúdo para transmissão adiante.¹³⁸
- A criação de 'assinaturas' digitais para conteúdo no ponto de transmissão. Estas seriam transmitidas juntamente com o conteúdo encriptado, permitindo que os prestadores de serviços online filtrassem as mensagens em busca de assinaturas ('hashes') de material conhecido de abuso sexual de crianças.^{139 140}

Nenhuma destas soluções facilitaria diretamente o acesso das forças da lei ao conteúdo: a polícia continuaria a exigir que os dispositivos dos suspeitos ou das vítimas fossem prova do crime.¹⁴¹ Ainda assim, estas soluções poderiam facilitar uma detecção e remoção mais proativa de material de abuso sexual de crianças, em oposição a uma intervenção apenas reativa, desencadeada pelos relatórios dos utilizadores ou pelas investigações policiais.¹⁴² Os defensores da privacidade poderiam argumentar que tais medidas seriam desproporcionais, uma vez que os benefícios da E2EE são mais relevantes do que a questão da exploração e abuso sexual de crianças online, para a maioria dos utilizadores da Internet.¹⁴³

A cooperação voluntária e a transparência são complementos essenciais para a regulamentação e necessários para manter coesa a resposta global.

Ao ajudar as empresas a contrabalançar o direito à privacidade com a segurança dos utilizadores, a regulamentação da Internet poderá mitigar parcialmente o impacto da E2EE na detecção de instâncias de abuso e exploração sexual de crianças online. As leis têm efeito potencial de melhorar a prevenção: o Canadian Centre for Child Protection considera a regulamentação como sendo determinante para a redução dos "altos níveis de reincidência das imagens" e os "longos atrasos nos tempos para a sua remoção", através da criação de incentivos comerciais e legais "para evitar que as imagens cheguem sequer a aparecer ou a ressurgir".¹⁴⁴

A implementação de novas leis para a Internet trará, indubitavelmente, desafios a vários níveis — representam um território desconhecido para muitos governos e levantam questões difíceis, como sejam:

- Como prevenir os danos sem restringir indevidamente a liberdade de expressão?
- O que constitui conteúdo "danoso" (conteúdo ilegal seria mais fácil de definir)?
- Como mitigar o risco de que as leis tenham um impacto comercial desproporcional nas empresas de menor dimensão?
- Para as empresas com uma base de utilizadores de diferentes nacionalidades, como garantir o cumprimento da regulamentação nas diferentes jurisdições?¹⁴⁵

A adaptabilidade e a colaboração estreita com os prestadores de serviços online serão essenciais durante a implementação das leis, para permitir que estas possam dar origem aos benefícios esperados.

Em última análise, será necessária uma solução global: um acordo internacional é a única forma de reduzir o risco de criar o que o Comissário do e-Safety da Austrália caracteriza como uma "splinternet" regulatória de diferentes leis entre países e regiões. Estas inconsistências globais podem prejudicar a eficaz supervisão,¹⁴⁶ devido ao facto de as empresas ou os próprios utilizadores da Internet adaptarem as suas atividades e comportamentos para escaparem à regulamentação. É possível que "à medida que as grandes plataformas reprimem... se dê um êxodo para espaços que são mais difíceis de examinar e moderar".¹⁴⁷ Já as bases de utilizadores de algumas das maiores plataformas parecem estar a diminuir. Globalmente, o tempo despendido nas cinco redes sociais mais descarregadas — as aplicações de redes sociais caiu 5% em 2020.¹⁴⁸

Entretanto, a cooperação voluntária e a transparência existem como complementos importantes à regulamentação. Para além de preencherem as lacunas emergentes entre os diferentes quadros regulatórios, a cooperação e a transparência permitem que exista uma capacidade de resposta para enfrentar uma ameaça em rápida evolução.

A transparência dos prestadores de serviços online é fundamental para melhorar a nossa compreensão da ameaça e daquilo que pode contribuir para uma resposta eficaz. À medida que as ferramentas de deteção e interrupção evoluírem tecnologicamente, a transparência será cada vez mais importante para estabelecer padrões consistentes para seu uso proporcional e para "aliviar os receios relativamente ao 'exacerbamento da missão' e ao uso indevido de tecnologia".¹⁴⁹

A cooperação voluntária internacional avançou (ver Figura 11) a par da inovação tecnológica. É necessário mais empenhamento para garantir que as iniciativas sejam geograficamente inclusivas e que envolvam uma ampla diversidade de partes interessadas com um papel na disponibilização de serviços online, por exemplo, indo além das plataformas para os fabricantes de dispositivos e operadoras de redes móveis de telecomunicações.

Figura 11: Exemplos de cooperação voluntária internacional.



O NCMEC registou uma redução de 58% nas denúncias recebidas através da Cyber Tipline na UE, aquando da descontinuação do seu uso por algumas empresas em dezembro de 2020, a fim de cumprir a diretiva europeia para a privacidade eletrónica.

Danos

Aliciamento online de crianças com vista à sua exploração e abuso sexual

À medida que mais crianças usufruem de um acesso crescente à Internet, existe um risco significativo de que a incidência do aliciamento online continue a aumentar, a menos que sejam implementadas soluções de proteção dos mais jovens.

Em 2020, o NCMEC reportou um aumento de 97,5% na "sedução online"¹⁵³ — uma ampla categoria de exploração que abrange o aliciamento online. Segundo o NCMEC, tal envolve "a comunicação de um adulto com alguém que se crê ser uma criança, através da Internet, com a intenção de cometer um crime sexual ou um rapto".¹⁵⁴

O inquérito de 2020 da Netclean que abrangeu 470 agentes da polícia de 39 países, revelou um aumento nas tentativas de contactar crianças, corroborando a inferência de que a incidência do aliciamento online está a aumentar.¹⁵⁵

O aliciamento pode, muitas vezes, propiciar todo um espectro de danos associados à exploração e o abuso sexual de crianças: a produção de imagens, a coação, a extorsão e o abuso presencial, cujas consequências podem ser graves. Um estudo do NCMEC sobre as denúncias de extorsão sexual registradas entre 2014 e 2016 revelou que, das vítimas que haviam experienciado um desfecho negativo, uma em cada três passou a ter comportamentos de automutilação e ameaça ou tentativa de suicídio.¹⁵⁶ Existem evidências de que o aliciamento online é uma prática também usada por traficantes para recrutar crianças para a exploração sexual com motivação comercial.¹⁵⁷

É difícil ir mais fundo na prevalência do aliciamento online porque muitos países ainda não definiram esse conceito na lei. Um exercício de benchmarking conduzido pelo Economist Impact, em 2020, para classificar as respostas dos países ao abuso sexual de crianças revelou que, dos 60 países estudados, apenas 21 dispõem de legislação que proíbe o aliciamento online para fins sexuais.¹⁵⁸ A ausência de uma definição legal tornam mais complicado o processo de denúncia e investigação tanto a nível local como internacional. O aliciamento encontra-se

tipificado como crime na "Convenção de Lanzarote" (a Convenção do Conselho da Europa para a Proteção das Crianças contra a Exploração Sexual e o Abuso Sexual — ver o Glossário de Termos).

Contudo, esta definição pressupõe uma proposta de encontro seguida de "atos materiais" conducentes a um encontro. A definição carece de atualizações para contemplar situações em que o abuso é perpetrado exclusivamente online.¹⁵⁹

As características do ambiente digital criaram novos fatores de risco de aliciamento online.

Um estudo de 2017 estimou que, aos 12 anos, 50% das crianças no mundo terá contas nas redes sociais —¹⁶⁰ uma "pegada digital" que "ajuda os predadores a mergulharem nas vidas das crianças como uma preparação para o contacto".¹⁶¹ As informações recolhidas através de recursos como a geo-referenciação das imagens e os "check-ins" nos lugares podem ser usadas pelos criminosos para ampliar o sentimento de encurralamento das suas vítimas, ou para permitir oportunidades para um agressor localizar fisicamente uma criança. Em certa medida, a Internet veio normalizar a comunicação com estranhos — o EU Kids Online Survey de 2020 concluiu que manter contacto com alguém desconhecido online é uma já experiência comum para 37% das crianças.¹⁶²

A Internet facilita táticas de aliciamento que não são replicáveis no contexto da realidade física:

"Para aqueles cuja intenção é explorar crianças, é muito mais fácil hoje, do que era há 20 ou 30 anos, lançar uma rede tão extensa quanto possível. É-lhe fácil enviar mil solicitações e, numa questão de dias, receber 999 recusas. Mas basta um pedido de amizade ou de conversa aceite, e abre-se a porta."

Thorn, abril 2021¹⁶³

Uma análise das denúncias em 'Online Coercion and Sexual Extortion of Children' registadas pelo NCMEC entre

2013 ————— **2016**

revelou o uso de múltiplas plataformas em

42%

de casos.



O modo como as crianças respondem nessas situações é uma função de uma complexa interação de fatores. Desde o início de 2020, estes fatores incluem a experiência individual da criança durante a pandemia de COVID-19. Como advertiu a instituição solidária britânica, NSPCC: “Os sentimentos de solidão provocados pelo contexto de pandemia levaram algumas crianças a procurar a companhia e o apoio de estranhos, o que as colocou em risco acrescido de serem aliciadas”¹⁶⁴

Os ambientes online oferecem diversas oportunidades àqueles que procuram aliciar outros.

Uma tática comum empregue pelos perpetradores de aliciamento online é a utilização de vários canais no intuito de aceder a um número mais amplo de potenciais vítimas, e evitar a deteção. Os infratores procuram sistematicamente migrar a conversa de uma plataforma pública para uma aplicação de mensagens privadas — uma técnica conhecida como "off-platforming". Normalmente, a interação é movida para aplicações que usam E2EE (garantindo que as comunicações não podem ser monitorizadas) ou para outras que não possuam ferramentas integradas para detetar comportamentos predatórios. Os infratores costumam migrar em grande número para plataformas mais recentes com mecanismos de segurança e moderação ainda pouco desenvolvidos. Uma análise dos relatórios de 'Coerção Online e Extorsão Sexual de Crianças' registrados pelo NCMEC, entre 2013 e 2016, revelou a utilização de várias plataformas em 42% dos casos.¹⁶⁵ O inquérito Economist Impact encomendado juntamente com este relatório concluiu que 68% dos entrevistados que receberam material sexualmente explícito online durante a infância, o receberam por via de um serviço de mensagens privadas.

As crianças relataram ter sido abordadas por "groomers" em redes sociais, aplicações de mensagens instantâneas, plataformas de transmissão ao vivo e serviços de chat de voz ou texto integrados em jogos multiplayer online".¹⁶⁶ As plataformas de jogos representam desafios complexos para a segurança infantil uma vez que, em tais ambientes, as interações entre adultos e crianças são relativamente normalizadas. A socialização nos jogos é facilitada pelo chat de áudio e vídeo integrados, sendo que plataformas permitem que os jogadores comuniquem ao vivo enquanto jogam. A Europol alertou que as crianças “estão mais expostas a potenciais infratores através dos jogos online”,¹⁶⁷ em parte, como resultado da pandemia COVID-19 a que foi atribuído o crescimento da indústria dos jogos, em 2021, ao ponto de exceder as previsões anteriores em 50%.¹⁶⁸

MARIE COLLINS FOUNDATION: A história da Olívia

A Olívia* foi alvo de aliciamento sexual online por parte de vários abusadores, durante um período de dois anos. A menina tinha 10 anos quando o abuso foi descoberto. O abusador principal aliciou-a através de uma aplicação de jogos para crianças antes de mover a conversação para aplicações mais privadas.

Mais tarde, o abusador partilhou os detalhes de Olívia com outros abusadores, que começaram a contactá-la diretamente, enviando-lhe links para vídeos pornográficos, com a intenção de normalizar o comportamento sexual e ensinar à menina o que ela deveria fazer.

Tratava-se de homens de vários países diferentes, que comunicavam através da "dark web". Olívia acabou por "revelar" o abuso ao deixar o seu dispositivo móvel desbloqueado, com os emails dos agressores abertos para que o seu pai visse. Olívia recebia centenas de

emails de homens diferentes e não conseguiu mais guardar o segredo.

Estava assustada e queria que este abuso parasse. A Fundação Marie Collins (MCF) é uma instituição solidária, sediada no Reino Unido, cuja visão é garantir que todas as crianças e jovens que sofram abuso sexual recebam apoio para a sua recuperação e vivam vidas gratificantes e em segurança.¹⁶⁹

*pseudónimo

A descoberta das "palavras dissimuladas" dos abusadores expõe ainda mais conteúdo danoso nas plataformas de jogos.



O anonimato e a natureza sem barreiras ou fronteiras da Internet, associados à facilidade de acesso a espaços percebidos como seguros online, confere aos perpetradores a confiança necessária para partilharem materiais de abuso sexual de crianças, e permite-lhes o uso de táticas e "tradecraft" para evadirem a deteção através de redes de criminosos.

Para a indústria dos jogos, as salas de chat, as chamadas de voz e o streaming ao vivo abriram vias para os abusadores chegarem ao contacto com as crianças e iniciarem os processos de aliciamento. A Crisp apresentou uma análise das conversas observadas na dark web que, mencionando três plataformas de jogos populares á escala global, revelou uma comunicação contínua entre abusadores em que estes, aparentemente, partilhavam dicas e conselhos relevantes sobre a prática do aliciamento.

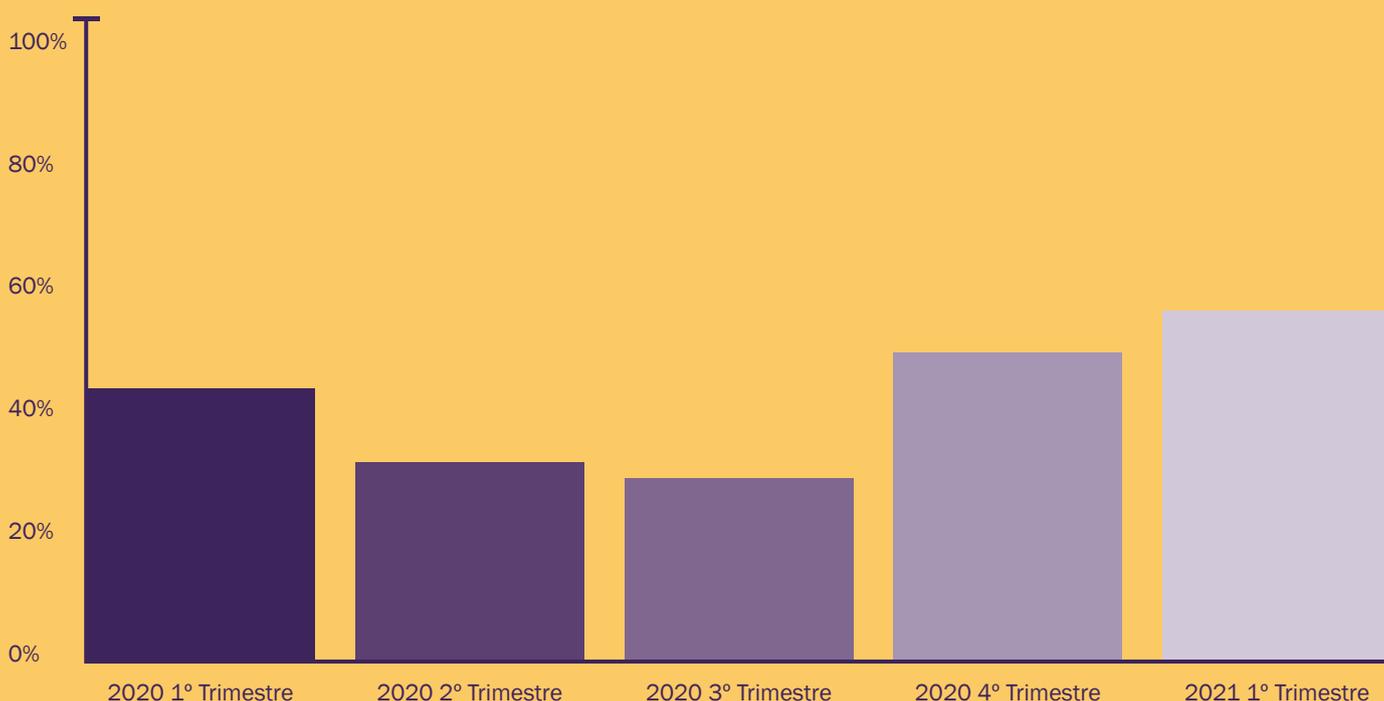
O número de conversas aumentou, em média, 13% em todas as plataformas entre 2019 e 2020. A Crisp observou ainda o uso recorrente de "palavras dissimuladas" pelos criminosos nas suas próprias

plataformas. Estas são palavras em que as letras-chave são substituídas por números ou símbolos para evitar métodos de deteção (por exemplo, digitar "8!Rthday" em vez de "Birthday", ou seja, "aniversário"). Através da identificação das instâncias em que os abusadores dissimulavam as palavras nas plataformas, a Crisp identificou até 50% mais peças de material contendo esse tipo de vocábulos, o que levou à identificação de conteúdos mais danosos e dos abusadores que os fomentavam.

A segurança do utilizador — em jogos ou em qualquer plataforma de rede social ou de conteúdo gerado pelo utilizador — exige a capacidade para identificar rapidamente qualquer conteúdo danoso, assim como as estratégias que assistem à sua criação. A aplicação no terreno destas estratégias de vigilância e investigação é essencial para a identificação dos perpetradores e para edificar as políticas a serem implementadas ou atualizadas no sentido de prevenir danos futuros.

Figure 12: Conteúdos adicionais encontrados quando foi identificado o vocabulário dissimulado.

Percentagem adicional de conteúdos que incluem termos-chave na pesquisa por termos dissimulados



As soluções para detetar o aliciamento online existem, mas a sua adoção não é generalizada e os desafios técnicos persistem. As ferramentas que usam inteligência artificial para identificar e bloquear conversas sobre aliciamento de crianças já estão postas em prática, contudo, apenas 37% das empresas que responderam a um inquérito da WeProtect Global Alliance /Technology Coalition implementaram estas tecnologias.¹⁷⁰

A deteção de aliciamento online apresenta vários desafios. A construção de ferramentas depende de os programadores terem acesso a "scripts" de chat para treinarem os algoritmos. Embora existam exemplos de colaboração eficaz entre a polícia, as plataformas e os programadores, existe espaço para afinar os processos de partilha de dados de modo a fomentar a inovação. Entre as dificuldades acrescidas, contam-se o desenvolvimento de ferramentas que funcionem em diferentes idiomas e lidar com o uso de gíria e palavras em código. A aposta na inovação contínua importa no sentido de aumentar a precisão das ferramentas tecnológicas, o que também minimizaria intrusões injustificadas na privacidade do utilizador.

As soluções mais eficazes são aquelas que podem detetar conversas de alto risco para evitar o aliciamento antes que ele aconteça. Esta tecnologia é complexa, no entanto, até porque "o teor das mensagens no chat pode escalar muito rapidamente... uma conversa pode tomar um rumo sexual em apenas três minutos".¹⁷¹ A maioria das ferramentas de deteção do aliciamento não são prontamente implementadas nos ambientes E2EE.

A incidência do aliciamento online pode ser significativamente reduzida tornando os ambientes online 'Safe by Design'.

'Safety by Design' é uma iniciativa do Australian e-Safety Commissioner, agora conhecido mundialmente, que determinou que a segurança do utilizador é "um princípio fundamental da concepção e que precisa ser incorporado no desenvolvimento das inovações tecnológicas logo desde o início".¹⁷²

As soluções "Safety by Design" com maior potencial para reduzir o risco de aliciamento online incluem a estimativa de idade e ferramentas de verificação de idade. Essa tecnologia é ainda relativamente incipiente,¹⁷³ mas poderia ser usada para excluir os predadores dos fóruns infantis e garantir experiências online que sejam adequadas à idade dos utilizadores mais jovens. Outros exemplos seriam os controlos parentais e os filtros de conteúdo. Muitas plataformas convencionais já incorporam alguns destes programas:

- A plataforma de jogos **Roblox** dispõe de um software de segurança integrado que bloqueia conteúdos explícitos e evita que os utilizadores jovens partilhem as suas informações de contacto.¹⁷⁴
- A plataforma de rede social **TikTok** introduziu configurações de privacidade e segurança de origem para os menores de 18 anos.¹⁷⁵
- **Instagram** está em processo de reforçar as funcionalidades de segurança para proteger os adolescentes das mensagens diretas indesejadas de adultos que não conhecem.¹⁷⁶
- **YouTube** desenvolveu aquilo a que denomina como "Experiências supervisionadas" para crianças menores de 13 anos, limitando a sua capacidade de enviar conteúdos, escrever no chat ou receber comentários, ajudando os pais a gerir o conteúdo ao qual as crianças conseguem aceder.¹⁷⁷

Estas funcionalidades podem contribuir para reduzir o risco de crianças serem vítimas de aliciamento online, limitando as oportunidades dos abusadores e educando as crianças sobre os riscos da Internet. Podem ainda reforçar a eficácia de outros mecanismos de segurança, reduzindo o volume geral da incidência e permitindo uma monitorização e proteção mais direcionadas.

YOTI: TECNOLOGIA DE ESTIMATIVA DE IDADE

A YOTI é uma plataforma de identidade global, baseada no Reino Unido, que aplica a tecnologia de estimativa de idade.

O mecanismo de IA da YOTI para a estimativa da idade, analisa o rosto da pessoa efetuando uma estimativa da idade em apenas 1 a 1,5 segundos, sem revelar ou reter quaisquer dados pessoais. Atualmente, este software apresenta uma taxa média de precisão de 2,19 anos em todas as idades, e de 1,5 anos para as idades dos 13 aos 25 anos — assegurando assim a moderação ajustada à idade estimada de acordo com os escalões de idade definidos no setor. É inclusivo para 13% da população global que não possui identificação com foto.

Até ao momento, a tecnologia de estimativa de idade do YOTI efetuou mais de 500 milhões de verificações de idade para organizações parceiras, nomeadamente em serviços de streaming ao vivo; comércio eletrónico; sites de adultos, jogos, e operadoras de telecomunicações.

É importante que melhoremos a nossa compreensão do fenómeno do aliciamento online de modo a propiciar uma prevenção e deteção eficazes e continuadas. A eficácia das intervenções pode ser limitada se as lacunas no conhecimento e na pesquisa não forem corrigidas.

Ainda não entendemos totalmente a interação entre o aliciamento online e "presencial" e as complexidades de intervir para prevenir que o abuso se dê, especialmente se o aliciador for uma pessoa conhecida da criança (como é o caso na maioria dos casos do aliciamento "presencial").¹⁷⁸ Ao mesmo tempo, existe a necessidade de melhorar a compreensão das vias de acesso daqueles que aliciam crianças online e de quais serão os fatores de risco e de proteção que influenciam as probabilidades de uma criança ser abusada. É sabido, por exemplo, que as crianças com deficiência podem apresentar vulnerabilidades específicas uma vez que recorrem à Internet para compensar a falta de apoios e/ou de conexões no mundo físico.¹⁷⁹ Os ensinamentos obtidos destas questões podem ser aplicados à concepção de modos de intervenção potentes e personalizados para melhor proteger as crianças e continuar eliminar ou reduzir as oportunidades de acesso do abusador.

Danos

Produção de materiais de abuso sexual de crianças

Quando o abuso de uma criança é documentado, o autor comete também o crime de produção de material de abuso sexual infantil.

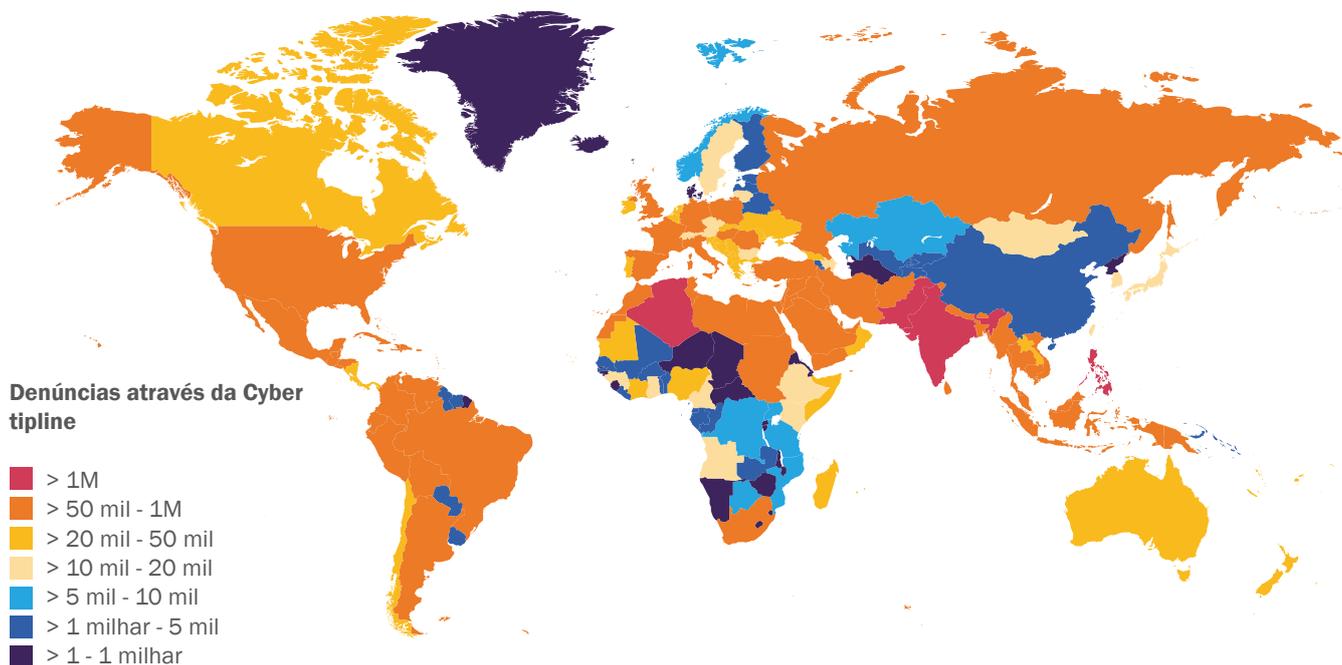
Os abusadores estão a evoluir nos seus métodos de produção, muitas vezes para tirar melhor proveito das novas tecnologias.

A produção deve ocorrer em todas as regiões do mundo. As meninas, de todas as idades, aparecem com mais frequência em imagens.

Um estudo conjunto da Thorn, Google e NCMEC, de 2019, revelou que 81% das denúncias de material de abuso sexual de crianças eram provenientes da Ásia, de África e da Europa.¹⁸⁰ A evidência mais recente do NCMEC (ver Figura 13 abaixo) indica que as mesmas regiões, com a adição das Américas, continuam a gerar uma grande parte das referências.

Infelizmente, esses dados oferecem uma visão intrinsecamente limitada das tendências globais. Exemplo disso é a origem dos relatórios poder não ser a mesma que a origem das imagens. Por outro lado, as denúncias transmitem apenas a extensão do problema "conhecido". É altamente provável que ocorra (mais) produção nos países onde há menos mecanismos (ou até nenhum) estabelecidos que a identifiquem. Isso mesmo é corroborado pelos resultados do inquérito Economist Impact, que revelou que as crianças sofrem danos sexuais online em todas as regiões do mundo.

Figura 13: Origem das denúncias de suspeita de exploração sexual de crianças recebidas através da linha Cyber Tipline do NCMEC em 2020. Reproduzido com autorização do NCMEC.¹⁸¹





Tornando claros os viesamentos geográficos em jogo, as evidências indicam que as crianças da América do Norte e da Europa Ocidental são mais propensas a serem identificadas em imagens de abuso do que crianças da Europa Oriental e do Sudeste Asiático, muito provavelmente devido a processos de denúncia e protocolos de identificação das vítimas mais avançados.¹⁸² Este padrão é sintomático das desigualdades mundiais que alteram o impacto local do abuso e mudam a forma da ameaça geral.

Em 2020, o INHOPE avaliou 267.192 URLs de conteúdo ilegal, dos quais 93% envolvendo crianças do sexo feminino.¹⁸³ A IWF, uma parceira próxima do INHOPE, relata a mesma proporção de conteúdo com meninas nos URLs avaliados pela sua equipa.¹⁸⁴ Isto não significa necessariamente que as meninas estão mais sujeitas a abusos do que os meninos. Na verdade, a pesquisa do Economist Impact identificou apenas uma ligeira diferença nas experiências relatadas pelos inquiridos do sexo masculino e do sexo feminino. O abuso de meninos pode, simplesmente, ser menos documentado. Isso pode sugerir, no entanto, que as meninas têm maior probabilidade de sofrer danos prolongados em resultado da produção, partilha e posterior distribuição das suas imagens.

O material de abuso sexual de crianças é frequentemente produzido por membros da própria família, o que levanta uma série de dificuldades na deteção e prevenção destas práticas. De acordo com a IWF, o material sexual infantil "autogerado" revela predominantemente crianças em ambiente doméstico.

¹⁸⁵ Apenas no ano passado, a maior produção em ambiente doméstico foi atribuída à adaptação dos grupos criminosos e dos seus modus operandi durante a pandemia de COVID-19, "aumentado o uso da comunicação online e das práticas de exploração dentro de casa".¹⁸⁶ No entanto, na maioria das vezes, as imagens são geradas dentro de casas de família porque os próprios membros da família são frequentemente os produtores do material de abuso sexual de crianças:

- Um estudo sobre casos de abuso sexual de crianças na Colômbia revelou que os criminosos fazem, normalmente, parte do círculo de confiança da criança ou da sua família nuclear.¹⁸⁷
- No México, 73% dos crimes de abuso sexual contra crianças são cometidos por familiares, sendo que 75% dos abusos ocorrem nas casas das vítimas.¹⁸⁸
- Na Austrália, um estudo com 150 adultos sobreviventes de abusos sexuais durante a infância revelou que 42% identificaram o próprio pai biológico, adotivo, ou o padrasto como o principal agressor e produtor de materiais de abuso de crianças.¹⁸⁹
- Um estudo de casos de abuso infantil, em Espanha, revelou que em 80,2% dos casos, o agressor pertencia ao círculo de confiança da vítima — sendo o pai biológico das crianças, em 32% dos casos.¹⁹⁰

US Department of Justice: website "BabyHeart" na Dark Web

"BabyHeart" era o nome de um site na dark web dedicado ao abuso de crianças com cinco anos de idade ou menos. Esteve disponível ao público por mais de dois anos, ao longo dos quais o número de membros cresceu para centenas de milhares. No website, os abusadores discutiam abertamente as suas preferências relativamente a crianças na faixa etária declarada uma vez que eram encarados como menos prováveis — ou incapazes — de denunciar o abuso, e eram considerados como sendo de "menor risco". A maioria das imagens partilhadas em "BabyHeart" foi, sem dúvida, produzida através de abuso no meio familiar ou em outros cenários de prestadores de cuidados. Esta situação constitui um forte alerta para a importância de mecanismos de prevenção e deteção que não dependam das denúncias serem feitas pelas próprias crianças e que não se pode presumir que as famílias são protetoras.¹⁹⁴

A infelicidade de sofrer abusos sexuais às mãos de um membro da própria família pode causar traumas adicionais e muito complexos, especialmente porque o abuso tende a iniciar-se em idades mais precoces na criança, e a prolongar-se por mais tempo.¹⁹¹ As vítimas de abuso familiar apresentam menor tendência para revelar ou denunciar as situações, pelo que as denúncias pelo próprio apresentem números baixos entre as vítimas de abuso sexual infantil. Apenas 2% das denúncias através da Cyber Tipline do NCMEC chega pela ação das próprias crianças.¹⁹²

Apesar dos avanços significativos no que respeita às tecnologias de análise de imagem e reconhecimento facial, as taxas de identificação de vítimas permanecem, de forma geral, baixas. Em abril de 2021, o Projeto Aracnid do Canadian Centre for Child Protection processou 126 mil milhões de imagens, 85% das quais mostram vítimas por identificar.¹⁹³ Os desafios da identificação de vítimas sublinham a importância crítica de educar comunidades inteiras e de investir em sistemas de proteção das crianças para conseguir melhorar a deteção dos abusos e para que as vítimas possam ser identificadas e salvaguardadas.

O Australian Centre to Counter Child Exploitation identificou o "capping" (captação ilícita de imagens) como a tendência atual mais problemática em termos do abuso sexual de crianças, que gera aproximadamente

60%-70%

de referências à sua Victim Identification Unit (unidade de identificação da vítima).

Em 2020, um "bot" de IA a operar no Telegram gerou

100,000

"deepfakes" pornográficos de meninas e mulheres reais.

Os métodos de produção de materiais de abuso e exploração sexual usados pelos abusadores estão a evoluir. Alguns são tão dissimulados que as crianças não se dão conta daquilo que estão a ser vítimas.

O "capping" (captação ilícita de imagens) tornou-se mais prevalente nos últimos anos, com algumas autoridades policiais a relatar um aumento acentuado durante a pandemia de COVID-19.^{195 196 197} Geralmente, as imagens envolvem aliciamento e coação sexual de crianças, sendo que esta prática está associada ao aumento da produção de material "autogerado" pelas crianças. Os abusadores abordam as crianças em diferentes plataformas, procurando conquistar a sua confiança, antes de as coagir a participar em atos sexuais que são captados em vídeo. O material é então partilhado nos fóruns da dark web. Segundo os dados da Europol, o número de mensagens e tópicos numa secção para "cappers" num fórum da dark web mais do que triplicou entre dezembro de 2019 e fevereiro 2020.¹⁹⁸

O Australian Centre to Counter Child Exploitation identificou o "capping" como a tendência atual mais problemática em termos do abuso sexual de crianças, gerando aproximadamente 60-70% dos encaminhamentos para Unidade de Identificação de Vítima daquela Polícia. O "capping" ilustra ainda o potencial de "gamificação" (consulte o Glossário de Termos) do abuso. Note-se o exemplo de um site na dark web, monitorizado pela polícia, organiza competições mensais e "batalhas de capping" nas quais os competidores se degladiam publicando imagens abusivas.¹⁹⁹

Embora algumas crianças saibam que foram vítimas de "capping", outras podem não ter consciência. A criação encoberta de material de abuso sexual de crianças é uma tendência de produção mais abrangente, facilitada por uma diversidade de dispositivos digitais, desde as webcams (às vezes, pirateadas) às câmaras de segurança de casa ou da escola. Na Coreia do Sul, o fenómeno é conhecido como "molka" e tem vindo a ser levado ao próximo nível com a implementação de câmaras espias em objetos do dia a dia como, por exemplo, canetas.²⁰⁰

A utilização de tecnologias como o CGI (Imagens Geradas por Computador) podem incentivar a diversificação da produção de conteúdos, pelo que exigem alterações à legislação existente.

De momento, as imagens de "deepfakes" e "CGI" não são geralmente encontradas em investigações de abuso de crianças.²⁰¹ Contudo, nada impede que se tornem mais populares. Em 2020, um "bot" de Inteligência Artificial, a operar no Telegram gerou 100.000 "deepfakes" pornográficas de mulheres e meninas reais.²⁰² Relacionado com este fenómeno, a indústria do cibersexo em realidade virtual registou um crescimento significativo, parcialmente atribuído ao impacto dos confinamentos da COVID-19.²⁰³ O Comissário Australiano para a Segurança Eletrónica (e-Safety) expressou a sua significativa preocupação relativamente ao uso potencial da realidade virtual e de outras "tecnologias imersivas" como "ferramentas para o abuso sexual de crianças online".²⁰⁴

Imagens Geradas por Computador (CGI – Computer-Generated Imagery) e "deepfakes"

O CGI é a criação de conteúdo visual estático (imagens) ou animado (vídeos) com software de tratamento e edição de imagem.²⁰⁵ No contexto do abuso sexual infantil, estamos a falar de imagens sexualizadas criadas parcial ou integralmente de modo artificial ou digital.²⁰⁶ "Deepfake" é uma forma de CGI que recorre à inteligência artificial (IA) para substituir a imagem de uma pessoa por outra em fotografia ou vídeo.²⁰⁷

As preocupações chave são as baixas barreiras à utilização e a natureza convincente dos resultados. Até mesmo os filtros mais simples integrados em aplicações populares são capazes de transformar o conteúdo com um simples clique. Alguns tipos de CGI podem criar dificuldades às Polícias no que toca à seleção das investigações uma vez que se torna difícil distinguir uma criança real de uma pessoa digital.²⁰⁸

O CGI e as tecnologias a ele associadas dificilmente poderão dominar o espaço cibernético, no atual estado das coisas, dada a abundância do material fotográfico de abuso sexual de crianças online. Ainda assim, devem ser tidos em conta até porque reiteram a necessidade de chegar a um acordo internacional sobre um conjunto de materiais não fotográficos que contribuem para a proliferação da ameaça, como sejam imagens por CGI, "deepfakes", animes, desenhos animados e ilustrações que retratam situações de abuso sexual de crianças, "bonecas sexuais" infantis, vendidas na Internet.

O CGI é danoso no sentido em que alimenta fantasias muito realistas, encoraja a propensão dos predadores sexuais e contribui para manter o mercado do material de abuso sexual de crianças".²⁰⁹ Existe ampla evidência que suporta esta posição, inclusive o facto de esse material ser frequentemente encontrado em conjunto com fotografias sexuais com crianças.²¹⁰ No entanto, muito poucos países consagraram o princípio na legislação.²¹¹

O CGI pode ainda ser utilizado para facilitar importantes técnicas de interrupção da atividade criminal, como aconteceu no caso "Sweetie" — uma persona infantil CGI foi utilizada para atrair e capturar mais de um milhão de predadores.²¹² Muitas redes de criminosos exigem que os candidatos a membros partilhem material novo para conseguirem obter acesso aos grupos fechados, pelo que filmagens artificiais são por vezes usadas pela polícia para conseguir infiltrar-se nessas comunidades. A colaboração entre Polícias a nível mundial é determinante para normalizar a utilização mais alargado deste tipo de táticas pelo que será necessário chegar a um consenso quanto às questões éticas relacionadas com a implementação desta tecnologia para tais finalidades.²¹³

Danos

Pesquisa por e/ou visualização de material de abuso sexual de crianças

Registam-se cada vez mais tentativas de acesso a materiais de abuso sexual de crianças. É fundamental atacar ambos os lados da questão, quer da "oferta" quer da "procura", para tornar sustentável a prevenção a longo prazo.

Grande parte do material de abuso sexual de crianças é acessado através da web de superfície, apps com E2EE e partilhas peer-to-peer (P2P).

Por vezes, bastam apenas três cliques para descobrir conteúdo de abuso sexual de crianças na Internet.²¹⁴ A maior parte do material é acessado dessa forma – via web de superfície ou por redes P2P.²¹⁵ De acordo com a Interpol, estas últimas foram as mais utilizadas até 2020.²¹⁶

Muitos indivíduos condenados por consumo de material de abuso sexual infantil demonstraram ter feito pouco ou nenhum esforço para encobrir o seu rasto,²¹⁷ ainda que esta amostra se possa considerar como sendo algo enviesada. Conforme destacado no Capítulo Temas: *Tecnologia*, uma parte dos infratores recorre a ferramentas e métodos avançados para evitar a deteção das suas atividades. Uma técnica documentada envolvia a criação de aplicações que direcionavam os utilizadores para grupos fechados de mensagens usados para partilhar imagens.²¹⁸ De acordo com a Europol, a distribuição de imagens de abuso sexual infantil “ocorre de forma rotineira em plataformas de redes sociais”.²¹⁹

Os abusadores costumam utilizar plataformas e aplicações E2EE, ambientes estes que combinam acessibilidade da web de superfície com um elevado nível de segurança. Conforme salientado na Avaliação de Ameaça ao Crime Organizado Grave de 2021 da Europol, “o uso generalizado de ferramentas de encriptação, incluindo aplicações E2EE, reduziu o risco de deteção” para aqueles que abusam sexualmente de crianças.²²⁰ A utilização de apps cria dificuldades significativas às forças da lei, uma vez que os agentes policiais precisam se infiltrar nos grupos fechados de mensagens para obterem provas da prática de abusos. Depois de conseguirem entrar, muitas agências policiais ficam limitadas à recolha manual de dados. A Child Rescue Coalition lidera atualmente o desenvolvimento de uma solução para agilizar a recolha de provas de crime nas apps de dispositivos móveis, em tempo real. A ferramenta foi

concebida para utilização por agentes da autoridade infiltrados nos grupos de criminosos. A redução da necessidade da recolha manual de dados aumentará significativamente a eficiência das operações secretas. A colaboração continuada entre as Polícias dos diferentes países é essencial para maximizar o impacto da ação policial e garantir uma melhor identificação e proteção das vítimas.²²¹

A dark web esconde os conteúdos mais extremos e permite a partilha e o networking das comunidades de criminosos.

Dark web

É a camada de informação e páginas que só podem ser acessadas através das chamadas “redes de sobreposição” (como as Redes Privadas Virtuais (VPN) e redes de partilha de ficheiros ponto a ponto (P2P)) que obscurecem o acesso público. Os utilizadores precisam de um software especial para aceder à dark web porque grande parte desta é encriptada sendo que o alojamento da maioria das páginas na dark web é anónimo.²²²

No seu conjunto, a atividade da dark web aumentou 300% nos últimos três anos.²²³ A dark web funciona, alegadamente, como um centro de distribuição de conteúdos mais jovens²²⁴ e mais extremos²²⁵ que retratam a exploração e o abuso sexual de crianças online.

As comunidades de criminosos na dark web vêm persistindo e evoluindo há mais de uma década. Nessa perspetiva, não representam propriamente uma nova dimensão da ameaça. O que mudou foi a maior disponibilidade de soluções de anonimato, como o Tor e os VPNs, agora tão comuns e até mesmo integradas de origem em alguns navegadores de Internet.²²⁶

Tor

"Tor" é uma rede de privacidade de código aberto que permite aos utilizadores navegarem anonimamente na Internet. O sistema utiliza uma série de nós em camadas para ocultar URLs, dados online e o histórico de navegação.²²⁷

Os utilizadores necessitam agora de conhecimentos técnicos mínimos para conseguir camuflar a sua atividade online. Para as autoridades policiais, o desafio é estar um passo à frente dos infratores que são mais hábeis na utilização desses recursos que garantem o anonimato e evitam que sejam apanhados.^{228 229 230}

O volume detentivas de acesso a materiais de abuso sexual de crianças continua a aumentar, sugerindo que existe uma associação entre a exposição regular a conteúdos sexuais extremos para adultos e a visualização de material de abuso sexual de crianças.

Em 2020, em apenas um mês, foram identificadas por três das organizações membros da IWF cerca de 8,8 milhões de tentativas de acesso e descarga de material de abuso sexual de crianças.²³¹

Durante os confinamentos por COVID-19, na Índia, registou-se um aumento de 95% nas buscas por material de abuso sexual infantil.²³² O Conselho de Direitos Humanos da ONU reportou igualmente que a procura de material de abuso sexual de crianças aumentou até 25% durante a pandemia, em alguns Estados-Membros da União Europeia.²³³

Numa estimativa conservadora, pensa-se que cerca de 1% da população masculina global seja afetada pela pedofilia (atração sexual por crianças pré-púberes).²³⁴ Muitos desses indivíduos procuram e visualizam material de abuso sexual de crianças,

conscientemente, para satisfazer os seus desejos sexuais.²³⁵ É imperativo que as forças policiais disponham de capacidades avançadas de policiamento para identificar os abusadores e gerir os riscos associados, inclusive a possibilidade de estes avançarem para cometerem abusos presenciais contra as crianças.

Existem muitos outros caminhos para a visualização de material de abuso sexual infantil. De acordo com a Lucy Faithfull Foundation, apenas 15% a 20% dos criminosos com que trabalham atualmente são pedófilos "para quem as crianças pré-púberes constituem o principal interesse sexual".²³⁶ Vários estudos estabeleceram uma ligação entre a visualização de material de abuso sexual de crianças e a exposição habitual a pornografia adulta extrema, supostamente, porque pode provocar uma dessensibilização erótica gerando o desejo de procurar estímulos mais severos para continuar a atingir o mesmo nível de excitação sexual.^{237 238} Duas áreas particularmente problemáticas são a chamada "pornografia temática de abuso"²³⁹ e a pornografia em que os adultos são retratados como crianças. O primeiro tipo torna mais fácil para os espetadores "darem o próximo passo para assistir a abusos reais", já o segundo foi descrito por infratores como uma porta de acesso ao material de abuso sexual de crianças.²⁴⁰

A ligação ao consumo de pornografia extrema é deveras preocupante, visto que a exposição das crianças a conteúdo sexual adulto aumentou drasticamente na era digital. Estudos realizados em vários países do Leste Asiático sugerem que 50% das crianças e jovens já foram expostos à "conteúdos sexualmente explícitos", enquanto os Estados Unidos, Austrália e vários países europeus reportam taxas de exposição de 80% ou mais.²⁴¹ A visualização frequente de pornografia adulta ou pornografia violenta desde uma tenra idade está associada à visualização de material de abuso sexual de crianças.

O modo como os utilizadores são levados a interagir com o conteúdo online contribui igualmente para acelerar os caminhos para o crime de abuso. O principal meio de impulsionar o envolvimento do utilizador nas plataformas das redes sociais é através da recomendação dos conteúdos. Em termos gerais, existem dois modelos para isto: o primeiro é o modelo algorítmico do "gráfico social", que presume os interesses do utilizador dando prioridade às atividades dos seus "amigos" e conexões sociais; o segundo é o modelo do "gráfico de interesse", que infere os interesses do utilizador com base em atividades anteriores e nas interações online. Para utilizadores que procurem conteúdo impróprio que envolva crianças, corre-se o risco de estes algoritmos incentivarem o comportamento abusivo, recomendando repetidamente imagens e vídeos similares.^{243 244} Tudo isto, combinado com contagens elevadas de visualizações de vídeo e tópicos de comentários perturbadores que muitas vezes escapam à atenção dos moderadores,²⁴⁵ tem o efeito global de facilitar a superação de inibições internas relativamente ao abuso.^{246 247} Algumas das principais plataformas afirmam dispor de mecanismos de deteção e de políticas de moderação que suportam a identificação de tais comportamentos.²⁴⁸ A oportunidade e a eficácia de tais medidas são fundamentais uma vez que, conforme explicado pelo National Centre for Social Research do Reino Unido, a "dessensibilização/perda de inibições online e a validação por parte de outros abusadores servem, muitas vezes, de motivação para visualizar material de abuso sexual de crianças e/ou realizar contactos abusivos".²⁴⁹

Bloquear as pesquisas por materiais de abuso sexual de crianças pode dissuadir o abuso, contudo, o impacto de tais intervenções é difícil de mensurar.

A comprovada ligação que existe entre a visualização dos conteúdo e o abuso presencial sublinha a razão pela qual a interrupção das tentativas de pesquisa por imagens é tão importante.

A maioria (60%) dos inquiridos numa investigação levada a cabo pela WeProtect Global Alliance /Technology Coalition confirmou que emite algum tipo de mensagem de dissuasão.²⁵⁰ A filtragem das pesquisas é um mecanismo popular usado principalmente pelos motores de busca. As consultas do utilizador são cruzadas com uma lista de conteúdos a serem bloqueados, pelo que, se a correspondência for estabelecida, nenhum resultado será apresentado. Em alguns casos, é também emitido um aviso para o utilizador. Após ter sido implementado pela Google e pela Microsoft, em apenas um ano, o número total de pesquisas feitas na web por imagens de abuso foi reduzido em 67%.²⁵¹

Um estudo financiado pelo governo australiano revelou que as mensagens de alerta online emitidas para os utilizadores que procurem ver "pornografia quase legal" aumentaram as taxas de diminuição até 25%.²⁵² Da mesma forma, a campanha "Stop it Now!" pela fundação Lucy Faithfull do Reino Unido e o projeto de prevenção Dunkelfeld, da Alemanha, demonstraram que a dissuasão pode promover a procura de ajuda nos (potenciais) abusadores.²⁵³ A Oak Foundation comprometeu-se, recentemente, a financiar um novo projeto de investigação para identificar e avaliar as iniciativas de prevenção dos comportamentos de abuso e ajudar a criar capacidade de implementação por meio de um hub online para legisladores e profissionais de saúde mental.²⁵⁴

A LUCY FAITHFULL FOUNDATION: A COLABORAÇÃO MINDGEEK (PORNHUB)

A Lucy Faithfull Foundation (a Fundação) é uma instituição de solidariedade social do Reino Unido que trabalha na prevenção do abuso sexual de crianças, desenvolvendo um trabalho de recuperação de adultos e jovens que cometeram abuso sexual ou que correm o risco de o cometer. Em fevereiro de 2021, a Fundação lançou uma colaboração com a Mindgeek para emitir mensagens de dissuasão no seu site de pornografia para adultos, o Pornhub. As mensagens são exibidas quando os utilizadores digitam buscas que indiciam tentativas de encontrar vídeos sexuais com crianças. A Mindgeek tinha já reconhecido a necessidade de exibir mensagens de dissuasão nos seus sites de conteúdos para adultos, onde detetou tentativas por parte de uma pequena minoria de utilizadores de pesquisa de material de abuso sexual de crianças utilizando termos de pesquisa banidos.

As mensagens de dissuasão recordam a lei, bem como os danos causados às crianças na criação e visualização desse material. Servem também para direcionar os utilizadores para sites ou mecanismos de apoio psicológico e de informação dissuasora de comportamentos ilegais — entre estes, a iniciativa "Stop It Now! Get Help", uma intervenção online autogerida para pessoas preocupadas com seu próprio comportamento sexual online em relação a crianças. Entre fevereiro e o início de maio de 2021, as mensagens de dissuasão trouxeram mais de 35.000 utilizadores de todo o mundo para a "Stop It Now! Get Help". Embora seja um número reduzido comparativamente com o volume geral de tráfego do Pornhub, conforme destacado pela Lucy Faithfull Foundation, este resultado revela bem a importância do papel que estas mensagens desempenham na educação e intervenção neste tipo de situações.

A principal dificuldade relativamente à dissuasão reside na medição da respetiva eficácia. Nos exemplos citados, essa medição foi possível através da monitorização das interações com materiais de ajuda e com os comportamentos de procura de ajuda — o que é limitado, até porque é impossível perceber se e em que medida a prática do crime terá sido efetivamente objeto de dissuasão. Subsistem igualmente dúvidas acerca do respetivo impacto de longo prazo: perceber se os utilizadores ficam dessensibilizados relativamente ao avisos ao longo do tempo, ou se, em vez disso, mudaram para outros sites e plataformas.

Os mecanismos de dissuasão são uma componente crítica de uma resposta mais ampla que incide sobre as diferentes vias de acesso ao consumo de material de abuso sexual de crianças.

É indiscutível a importância dos esforços de remoção do material de abuso sexual infantil da Internet. Contudo, se não existir um trabalho com os (potenciais) abusadores, no sentido de gerir a "procura", existirá sempre o risco de os indivíduos persistirem na pesquisa de novas formas de acesso às imagens, evitando a deteção. A importância de equilibrar os esforços entre a "oferta" e a "procura" é exemplificada por uma iniciativa atual da IWF. Responsável pela remoção de 153.600 páginas de abuso sexual infantil, só no ano de 2020,²⁵⁵ a organização uniu-se à Lucy Faithfull Foundation, e contando com o apoio da End Violence Partnership, para desenvolver o chatbot ReThink. A ferramenta irá interagir com os utilizadores que evidenciem comportamentos de pesquisa de material de abuso sexual infantil, sinalizando os serviços de apoio para que estes tentem dissuadir o comportamento antes que o mesmos se converta em crime.²⁵⁶ De uma perspectiva social mais ampla, as iniciativas de dissuasão são importantes no sentido em que “estão focadas na mudança do comportamento de adultos”, e não de crianças, e ao fazê-lo passam “uma importante mensagem sobre a quem compete a responsabilidade de prevenir o abuso sexual de crianças”.²⁵⁷

SUOJELLAAN LAPSIA RY: PROJETO REDIRECTION

Suojellaan Lapsia Ry é uma organização não-governamental finlandesa que ajuda a proteger crianças em todos os ambientes, através de programas de defesa, pesquisa e formação.²⁵⁸

O projeto ReDirection desta ONG, apoiado pela End Violence Partnership, foi lançado em setembro de 2020 e estender-se-á até setembro de 2022. Trata-se de uma iniciativa de investigação para recolher informações destinadas a orientar o desenvolvimento de novas e melhores formas de deter e impedir a prática criminal. A pesquisa envolve a distribuição de um questionário com 30 perguntas, denominado "Ajude-nos a ajudá-lo", através do motor de pesquisa "Ahmia" da dark web, que processa cerca de 20.000 pesquisas por dia. Ao longo de três meses, o questionário foi lançado automaticamente em resposta a mais de 20.000 pesquisas de material de abuso sexual infantil. Foram devolvidos mais de 3.

100 questionários preenchidos. Com base nos resultados da pesquisa, Suojellaan Lapsia planeia criar um novo programa de autoajuda para indivíduos que procuram e consomem material de abuso sexual de crianças. O objetivo é identificar os indivíduos em risco de infração e encaminhá-los para serviços de ajuda e apoio.

Ampliar a nossa compreensão dos caminhos que conduzem ao consumo de material de abuso sexual de crianças será a chave determinante para garantir eficácia da resposta a este tipo de ameaça. Este capítulo explorou apenas duas motivações relevantes: o interesse sexual em crianças e a dessensibilização causada pela exposição habitual a conteúdo sexual extremo. Mesmo as intervenções de dissuasão altamente eficazes têm baixas probabilidades de dissuadir os indivíduos mais determinados, daí a importância de desenvolver mecanismos de policiamento para identificar abusos persistentes e potencialmente mais sofisticados. Da mesma forma, torna-se claro que procurar uma resolução no âmbito da justiça criminal não é uma estratégia apropriada nem sequer exequível para dar resposta ao volume crescente dos crimes de visualização associados à dessensibilização e desinibição online.

Danos

Partilha e/ou retenção de material de abuso sexual de crianças

O volume de material de abuso sexual infantil disponível online é crescente. Os métodos de partilha e armazenamento de conteúdo estão cada vez mais evoluídos.

Entre 2019 e 2020, o número de denúncias chegadas através da linha Cyber Tipline do NCMEC relativamente a materiais de abuso sexual de crianças aumentou 63% no cômputo geral.²⁵⁹ No mesmo período, a IWF observou também um aumento de 16% nas denúncias confirmadas desse tipo de material tanto na web de superfície como na dark web.

O número inclui denúncias recebidas por parte de utilizadores dos serviços, assim como a deteções feitas pela equipa da IWF no decorrer de pesquisas ativas na Internet. Estes dados parecem indicar que o volume do material de abuso sexual de crianças atualmente disponível online tem vindo a aumentar.²⁶⁰

Globalmente, uma grande proporção dos relatórios diz respeito às partilhas de material "conhecido" (por oposição à "primeira geração" — ver as definições abaixo). A rede internacional INHOPE de linhas telefónicas de apoio direto para denúncias estima que 60% do conteúdo sinalizado em 2020 era "conhecido".²⁶¹

Material "conhecido" e de "primeira geração"

Material de abuso sexual de crianças referido como "conhecido" é aquele que já tinha sido previamente identificado e classificado pelas autoridades policiais e/ou pelos moderadores dos sites. O material de "primeira geração" é um conteúdo "novo" não detetado nem classificado anteriormente.

O material em vídeo é responsável por uma proporção crescente dos conteúdos detetados: o número de ficheiros de vídeo denunciados ao NCMEC aumentou dez vezes entre 2017 e

2020 (Figura 14). No mesmo período, o número de ficheiros de imagem duplicou. Atendendo a que muitas agências policiais e de moderação não têm largura de banda suficiente para processar imagens, essa tendência poderá enviesar a eficácia da deteção, a menos que os recursos sejam melhorados — em especial porque a capacidade de armazenamento nos dispositivos continua a aumentar.²⁶²

Os repositórios de imagens são o tipo de site mais usado para partilhar material de abusos sexuais de crianças.²⁶⁴ Estes incluem plataformas de redes sociais que são habitualmente usadas para disseminar material através de contas falsas que são rapidamente excluídas.²⁶⁵ Atualmente, não existe um mecanismo formal definido para que as plataformas partilhem legalmente os identificadores associados a essas contas, o que permite que os abusadores alternem livremente entre plataformas e serviços, operando com relativa impunidade.²⁶⁶

O uso de "serviços ocultos" para distribuição de material de abuso sexual de crianças aumentou 155% entre 2019 e 2020.²⁶⁷ Estes são sites alojados em redes proxy (como "Tor" — Ver o Glossário de Termos), de tal forma que sua localização não possa ser rastreada.²⁶⁸

Enquanto que alguns infratores continuam a acumular material em dispositivos como laptops, telemóveis e pen drives,²⁶⁹ notam-se sinais de afastamento da curadoria de coleções pessoais, com os abusadores a preferirem o acesso "on-demand" ao conteúdo através de sites de "alojamento de ficheiros";²⁷⁰ serviços de Internet que permitem aos utilizadores fazerem o upload de ficheiros para acesso remoto.²⁷¹ Os links para os ficheiros de conteúdo sexual infantil são publicados depois em diversos sites e frequentemente usados como parte das partilhas peer-to-peer.

Isto cria uma série de desafios às autoridades policiais. O material é frequentemente publicado e alojado em diferentes jurisdições, o que complica a recolha das provas do crime.²⁷² O volume dos conteúdos na posse de um abusador vem sendo, historicamente, um dos vários fatores tidos em conta na avaliação do nível de risco representado por essa pessoa, mas deixou de ser um indicador relevante.²⁷³

As aplicações de partilha na nuvem alimentaram uma explosão de interações dos utilizadores com conteúdo danosos.



As populações de abusadores passaram a poder contar com a facilidade de utilização, a segurança e a privacidade das aplicações de partilha na nuvem para o armazenamento e distribuição de imagens e vídeos ilegais. O armazenamento na nuvem torna possível a partilha de material de abuso sexual de crianças pelo simples gesto de publicar um link num fórum, numa qualquer plataforma ou através de mensagens privadas, chegando assim a mais abusadores, mais rapidamente.

A análise da Crisp mostra que instâncias de envolvimento dos utilizadores ou as interações com conteúdo danoso associadas ao abuso e exploração sexual de crianças registaram um aumento exponencial para quase 20 milhões no primeiro trimestre de 2021 — um aumento de mais de 5,5 milhões apenas no primeiro trimestre de 2020.

Nos cinco trimestres que medeiam entre janeiro de 2020 e março de 2021, a Crisp avaliou 1340 itens com links de partilha de conteúdo considerados de alto risco atendendo ao contexto e às comunidades em que foram partilhados. Onde existia um link danoso no conteúdo, o número de interações variou entre as 20 e as 12.746, nos casos mais extremos. A partilha em múltiplos locais e fóruns aumentou globalmente muito o número total de interações dos utilizadores com esses links.

Os autores recorrem normalmente à partilha de ficheiros na nuvem para trocarem imagens e vídeos, de forma eficiente com os seus contactos de abusadores, novos e conhecidos. Para garantir que o conteúdo permanece acessível pelo maior espaço de tempo possível, há quem utilize várias plataformas na nuvem em simultâneo. A verdadeira natureza dos links danosos está escondida atrás de uma cortina de fumo de referências a outras atividades ilegais (menos graves) ou à partilha legítima de ficheiros, de modo a evadir a deteção.

Figura 15: Interações dos utilizadores com conteúdo danoso.

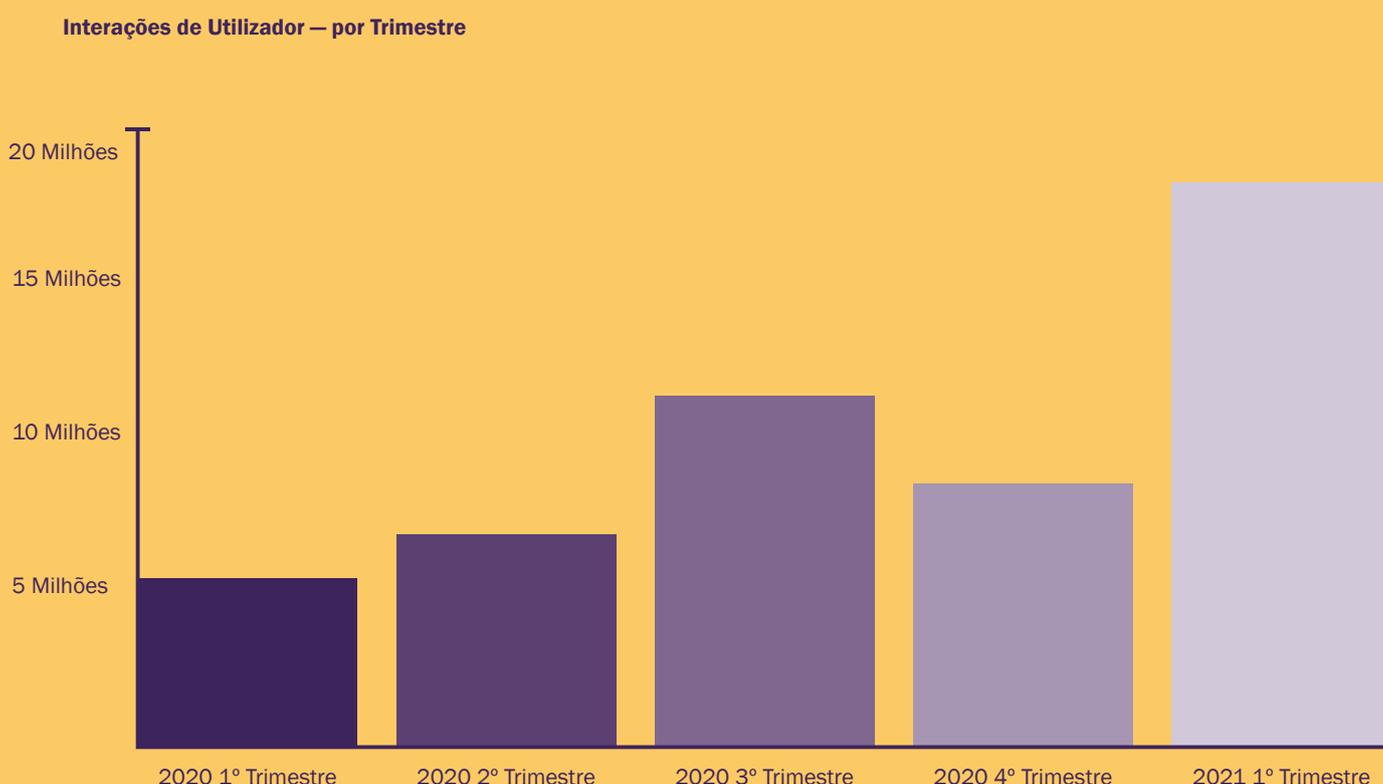


Figura 14: Aumento de material fotográfico vs material de vídeo, com teor de abuso sexual de crianças, reproduzido com autorização da NCMEC.²⁶³

Dados das tendências NCMEC: Aumento dos materiais de imagem e vídeo sobre abusos sexuais de crianças		
Ano	Imagens	Vídeo
2020	33,6 Milhões	31,6 Milhões
2019	27,7 milhões	41,2 Milhões
2018	23,2 Milhões	22,2 Milhões
2017	17,0 Milhões	3,4 Milhões

De todas as formas, a partilha repetida “serve para revitimizar e, portanto, exacerbar ainda mais o dano psicológico ao abusado”, muitas vezes evitando a resolução do trauma, até mesmo nos casos em que o abusador é apanhado e punido.

A partilha repetida de materiais ilegais está a agravar os danos provocados pelo abuso sexual de crianças.

Uma parte significativa das denúncias de material de abuso sexual infantil é gerada pela partilha de imagens "conhecidas". O Facebook declarou que mais de 90% das denúncias para o NCMEC, entre outubro e novembro de 2020, diziam respeito a partilhas ou reencaminhamento de partilhas de conteúdos já detetados anteriormente.²⁷⁴ Um estudo das denúncias feitas ao NCMEC, registadas entre 2011 e 2014, revelou que, de uma amostra de 2598, as imagens eram "ativamente comercializadas" (tinham sido denunciadas ao NCMEC cinco ou mais vezes) envolvendo, em 7% dos casos, apenas um abusador e uma vítima, e, em 12% dos casos, envolvendo múltiplas vítimas e /ou abusadores.²⁷⁵ Em todos os casos, a partilha repetida "serve para revitimizar, ou seja, exacerbar o dano psicológico ao abusado",²⁷⁶ muitas vezes evitando a resolução do trauma, mesmo nos casos em que o infrator é apanhado e punido.²⁷⁷ À medida que a partilha online prolifera, o uso de políticas de notificação de vítimas em regime de "opt-in" (tal como existem nos EUA) será cada vez mais determinante para garantir que os danos não sejam involuntariamente reiterados de cada vez que as imagens de um sobrevivente são redescobertas pela polícia ou agências de denúncia.²⁷⁸

Outras questões relacionadas com o reencaminhamento de partilhas são, por exemplo, o assédio e a perseguição de vítimas específicas, uma atividade que confere aos abusadores oportunidades de estabelecerem conexões com indivíduos com o mesmo tipo de comportamento.

O Facebook declarou que mais de

90%

das denúncias que apresentou junto do NCMEC, entre outubro e novembro de 2020, diziam respeito a partilhas ou reencaminhamento de partilhas de conteúdos já detetados anteriormente.

Um estudo das denúncias efetuadas ao NCMEC, registadas entre 2011 e 2014, revelou que, uma amostra de

2.598

imagens que eram "ativamente comercializadas" (tinham sido denunciadas ao NCMEC cinco ou mais vezes)

Os criminosos voltam a traumatizar os sobreviventes recorrendo a perfis falsos.



Usando uma tática que revitimiza os sobreviventes do abuso e exploração e sexual de crianças, os abusadores estão a criar perfis falsos online, nos quais se apropriam das identidades dos sobreviventes seus conhecidos. Essas contas fraudulentas, que normalmente adotam os nomes dos sobreviventes e apresentam imagens não danosas ao nível da conta /perfil, aparecem na web de superfície em várias plataformas de redes sociais.

As contas são usadas pelas comunidades de abusadores para se conectarem com outros abusadores, principalmente para trocaram informações de contactos. Isto pode levar também a que, em espaços online considerados seguros, os abusadores estejam a troca de táticas de exploração comercial dos materiais de abuso sexual de crianças e "tradecraft".

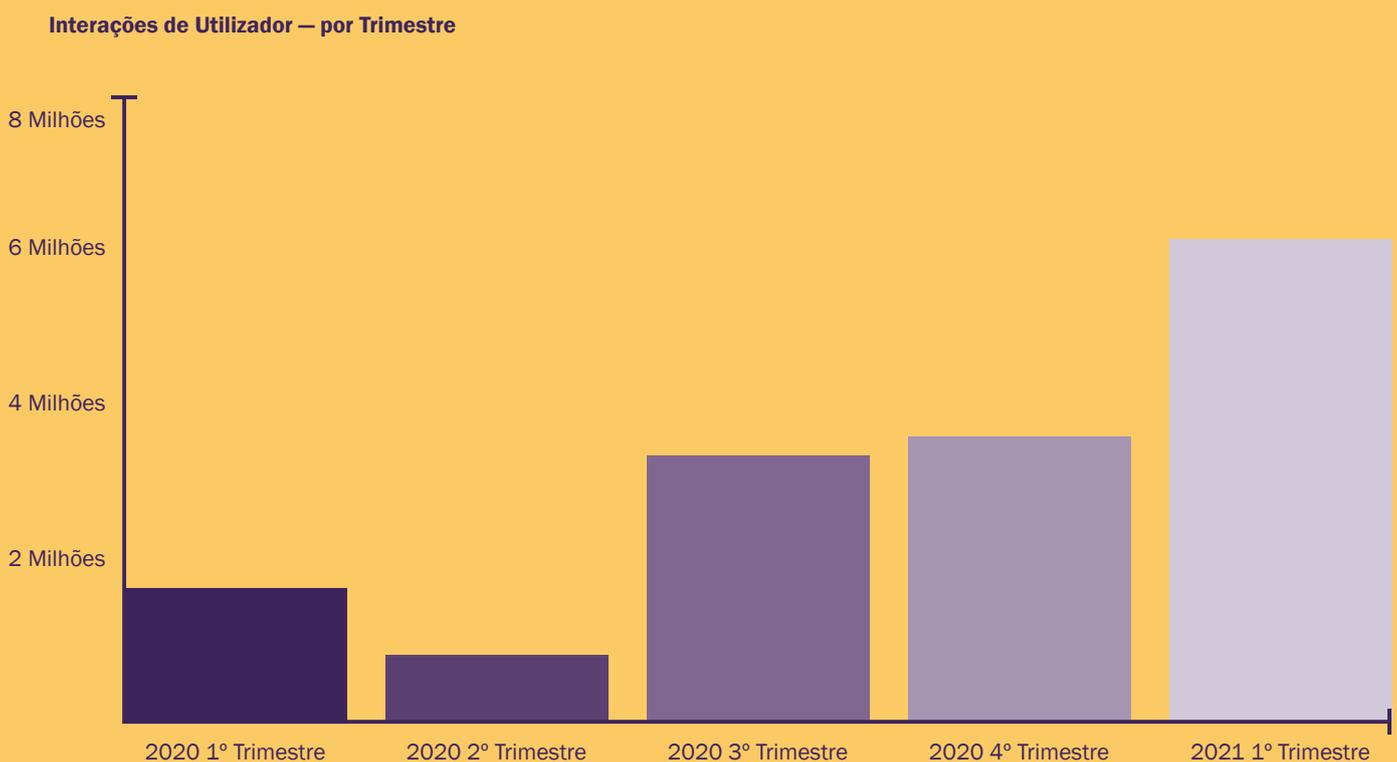
Cada vez mais abusadores estão a recorrer a estas contas para transmitirem publicamente as suas preferências ou interesses, e endossar sites comerciais que distribuem imagens abusivas.

Sendo uma tendência perturbadora, a Crisp observou a triplicação do número das interações de utilizadores com perfis falsos desde o primeiro trimestre de 2020 até o primeiro trimestre de 2021.

Por exemplo, entre janeiro de 2020 e março de 2021, a Crisp identificou 3324 peças de conteúdo que referiam sobreviventes conhecidos ou sites comerciais. Em média, cada conteúdo danoso gerou mais de 2000 interações (gostos, comentários, etc.), causando um efeito multiplicador e alcançando muito mais abusadores interessados.

A maior parte das referências incluía as conversas do abusador e a confirmação do consumo de material de abuso sexual de crianças. A maioria das referências ao material estava ligada a crimes perpetrados mais de uma década antes da criação dos perfis falsos. Esse recordatório de abusos sexuais anteriores tem o efeito de voltar a traumatizar os sobreviventes que, novamente, experimentam a perda do controle sobre as suas identidades, conforme publicadas nas redes sociais.

Figura 16: Interações dos utilizadores com conteúdos que referenciam sobreviventes conhecidos ou sites comerciais.



NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN (NCMEC):

A história da Ella

A Ella* foi abusada sexualmente por um membro da família desde os cinco anos de idade, e ao longo de sete anos. O agressor de Ella fez imagens e vídeos do abuso e distribuiu-os online. O NCMEC rastreou a localização do abuso, identificando-a como sendo numa região do oeste dos Estados Unidos, encaminhando o caso para as autoridades locais. A polícia localizou e resgatou a jovem Ella, sendo o abusador julgado e condenado.

Ainda que o criminoso esteja agora na prisão, as imagens e vídeos de Ella continuam a circular na Internet, pelo que outros criminosos continuam a assediá-la online. O cuidador da menina descreveu o trauma provocado pela partilha repetida dos conteúdos dizendo que "existe essa sensação de que o agressor vai para a prisão e é o fim. Mas não é... No início, senti-me estranhamente grato pela identificação das fotos, porque foi isso que permitiu apanhá-lo. Só que as imagens continuam por aí, não desaparecem. Já dezenas de milhares de pessoas a viram... até mesmo 10 anos mais tarde".

Ao longo dos anos, Ella recebeu milhares de notificações de vítimas do governo sobre casos envolvendo as suas imagens e vídeos. Mesmo na idade adulta, essa nova vitimização deixou Ella com necessidade de terapia contínua.

Ella usa agora a sua experiência para ajudar outras pessoas. Ela colabora como consultora de sobreviventes, contribuindo com a sua experiência para o desenvolvimento dos recursos de apoio do NCMEC e para a criação de novos programas de apoio a sobreviventes.

O Centro Nacional para Crianças Desaparecidas e Exploradas (NCMEC) é uma entidade privada sem fins lucrativos. A sua missão é localizar crianças desaparecidas, combater a exploração sexual infantil e prevenir a vitimização das crianças.

*pseudónimo

O Facebook analisou instâncias de partilhas entre 2019 e meados de 2020, concluindo que 75% deste material era "não malicioso". De acordo com a taxonomia do Facebook, estas são partilhas alegadamente motivadas pela indignação, tentativas de ridicularização ou numa ótica de vigilância.²⁷⁹ Seria de grande utilidade a imposição de maior transparência na classificação das partilhas "não maliciosas" e da taxonomia aplicada por outras plataformas no sentido de moldar estratégias que contrariassem esta tendência. Uma abordagem proativa por parte dos prestadores de serviços online seria a chave para combater este tipo de comportamentos e mitigar o risco da normalização, ou até banalização, do abuso sexual de crianças online.

O material de abuso sexual infantil está a ser distribuído com fins de ganho financeiro. Este tipo de partilha cria desafios únicos à sua deteção.

De acordo com a IWF, embora a percentagem de páginas comerciais da web, contendo material de abuso sexual de crianças tenha diminuído ligeiramente (-4%) relativamente ao ano anterior,²⁸⁰ a maioria dos domínios analisados em 2020 (61%) eram de natureza comercial.²⁸¹ A IWF continuou a observar novas modalidades de monetização dos conteúdos, como sejam os esquemas de afiliados que permitem aos editores ganhar dinheiro de cada vez que um link é clicado para aceder ao material abusivo.²⁸²

Observou-se também um aumento dramático no registo da utilização de criptomoedas para comprar material de abuso sexual de crianças. O valor total dos pagamentos de Bitcoin e Ethereum para endereços vinculados a fornecedores desses conteúdos foi de 930.000 dólares em 2019 — um aumento de 212% relativamente a 2017.²⁸³ Esta tendência tem correlação com o aumento da utilização de serviços comerciais ocultos para aceder aos conteúdos. A proporção de tais serviços tem vindo a aumentar desde 2016.²⁸⁴ sendo que as criptomoedas são o único método de pagamento aceite.²⁸⁵

A partilha comercial pode representar desafios extraordinários, já que os distribuidores costumam implementar táticas para frustrar as tentativas de deteção e remoção das imagens. Em 2020, observou-se um aumento dos "sites comerciais disfarçados". Estes sites evitam a deteção exibindo imagens ilegais apenas quando o site é acedido através de um "caminho digital" específico constituído por links de outros sites. Outros sites comerciais utilizam técnicas como o "top level domain hopping" (salto para domínios de nível superior) garantindo que os conteúdos sobrevivem online após o site original ter sido removido. O site altera o nome do domínio, mas mantém o seu nome de marca, para que os utilizadores continuem a localizá-lo.²⁸⁶

Mais inovação e uma maior adoção de ferramentas são necessárias para detetar o material e impedir a partilha deste.

A deteção eficaz de material "conhecido" de abuso sexual de crianças é possibilitada através de duas técnicas vinculadas chamadas "hashing" e "hash-matching". Estas técnicas aceleraram significativamente a identificação e a remoção de material abusivo da Internet.

"Hashing" e "hash-matching"

"Hashing" é um processo usado para transformar dados de qualquer dimensão em dados de comprimento fixo muito mais curtos. A sequência mais curta representa os dados originais e torna-se a assinatura exclusiva do ficheiro ou o seu "valor de hash".

"Hash-matching" é o processo pelo qual os hashes de reconhecido material de abuso sexual de crianças mantido em bases de dados são comparados com o "hash" de material recém-descoberto para determinar se o conteúdo já foi denunciado às autoridades. Se esse for o caso, o processo de remoção do conteúdo é geralmente simplificado e, muitas vezes, automatizado.²⁸⁷

Existem várias bases de dados para facilitar o "hash-matching". Uma das mais relevantes é a da Interpol, que conserva mais de 2,7 milhões de "hashes" de material de abuso sexual de crianças e é usada por 64 forças policiais em todo o mundo.²⁸⁸ Outras bases de dados disponíveis são a Child Abuse Image Database do Reino Unido, a lista de hash da IWF e o sistema da CyberTipline do NCMEC.¹

O método de "hash-matching" apresenta algumas limitações. Quando são detetadas imagens "conhecidas", a sua remoção depende da identificação do host para emitir um aviso de eliminação. Por vezes, surgem dificuldades em rastrear a localização do servidor que aloja o site, o que pode atrasar a remoção dos conteúdos.²⁸⁹ Em alguns países, a não conformidade com avisos de remoção constituiu um problema adicional.²⁹⁰ Seria fundamental implementar a colaboração estreita e contínua entre os governos, a indústria digital e as Polícias em todo o mundo, para garantir a eficácia permanente.

A adoção mais ampla da tecnologia é a chave para aumentar o seu impacto: embora a maioria dos inquiridos num estudo da Alliance/Tech Coalition tenha confirmado que usam "hash-matching" para imagens (87%) e vídeo (76%) para remover proativamente o material de abuso e exploração sexual de crianças das respetivas plataformas,²⁹¹ muitas organizações ainda não contribuem com "hashes" para bases de dados existentes, nem para a referência cruzada.²⁹²

A fusão das listas de hashes existentes poderia simplificar os esforços de deteção e remoção dos materiais ilícitos. Contudo, este esforço é obstaculizado pelas diferenças no modo de classificação do material adotado em cada país. A Interpol aplica uma etiqueta de baseline ao material que é ilegal em todos os países, que é usada por muitos de seus parceiros nas forças de segurança.²⁹³ Mas é mais difícil alcançar um consenso global sobre a classificação de imagens de menor gravidade. Com a junção de mais países seria possível melhorar a deduplicação e a deteção para aumentar significativamente o impacto generalizado da tecnologia.^{294 295}

A deteção e remoção de material de abuso sexual infantil de "primeira geração" apresentam um conjunto diferente de desafios. Existem soluções para detetar novos conteúdos, mas ainda são relativamente menos maduras e mais complexas do que o "hash-matching". Os chamados "classificadores" de conteúdo usam algoritmos informados por "machine learning" para identificar e categorizar os materiais de abuso sexual infantil. As dificuldades relacionadas com estimar as idades das crianças nas imagens²⁹⁶ e assim avaliar a sua gravidade significa que os classificadores tendem a gerar uma taxa de falsos positivos mais alta do que por "hash-matching", aumentando a necessidade da moderação humana.²⁹⁷ Será imprescindível uma maior inovação tecnológica para melhorar as taxas de precisão, reduzir a carga sobre os moderadores e permitir uma adoção mais alargada dessas soluções eficazes e seguras. Também haverá que continuar o trabalho de investigação para perceber de que forma os classificadores e o "hash-matching" podem funcionar eficazmente com a E2EE.

GOOGLE: CONTENT SAFETY API

Content Safety API é uma ferramenta desenvolvida pela Google, fornecida gratuitamente a ONGs e empresas privadas como apoio aos seus esforços de proteção das crianças. Recorre a inteligência artificial para ajudar as organizações a priorizar de forma mais eficiente as imagens potencialmente abusivas para análise humana, cujo o conteúdo não seja ainda "conhecido" enquanto material de abuso sexual de crianças. A identificação mais célere de novas imagens aumenta o ritmo a que as vítimas de abuso podem ser identificadas e protegidas. A eficaz definição de prioridades contribui igualmente para reduzir a pressão sobre os moderadores e verificadores.

A ferramenta já processou mais de dois mil milhões de imagens, ajudando empresas como Yubo, Plugon e Facebook, bem como ONGs como a Safernet Brasil, a melhorar a deteção e a denúncia de material de abuso sexual de crianças.

06 Danos

Material sexual "autogerado" pela criança

O volume de material sexual "auto-gerado" pela criança aumentou durante a pandemia de COVID-19.

O material sexual "auto-gerado" pelas crianças apresenta uma componente crescente de abuso sexual de crianças. Tal cria desafios complexos para os legisladores, e exige uma resposta multifacetada.

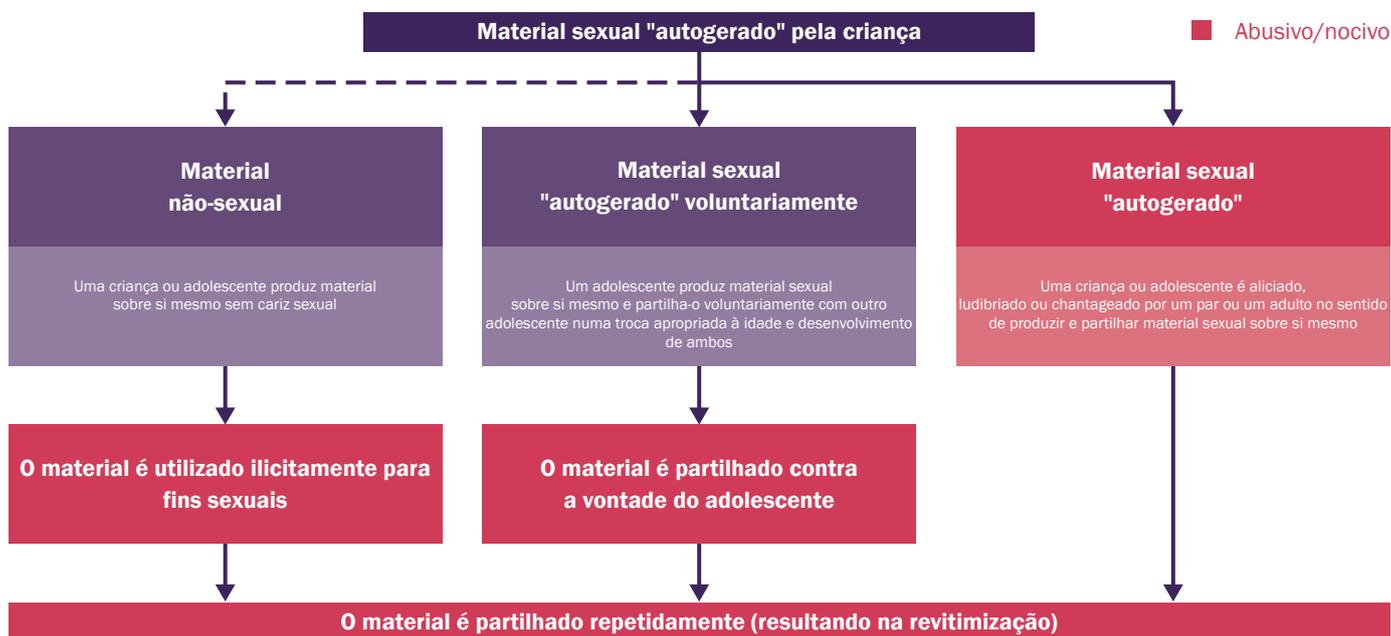
A IWF apresentou um "estudo instantâneo" do conteúdo "autogerado" no respectivo Relatório Anual de 2012.²⁹⁸ Em 2017, a ECPAT descreveu este tipo de conteúdo como uma "tendência atual"; atribuindo o volume crescente de material "autogerado" à qualidade comercializada das imagens "recém-produzidas, nunca antes vistas", o que faz delas uma "moeda" valiosa para os abusadores.²⁹⁹

Mais recentemente, o volume de material "autogerado" aumentou drasticamente.

A IWF recebeu 68.000 denúncias de material sexual "autogerado" em 2020, um aumento de 77% em relação a 2019. No conjunto, os conteúdos "autogerados" corresponderam a 44% de todos os relatórios acionados pela IWF em 2020.³⁰⁰

Essa escalada atribuí-se, em parte, à "tempestade perfeita" criada pela pandemia da COVID-19: as crianças passam mais tempo online, enquanto que a redução das oportunidades para cometer o abuso presencialmente alimentam os abusos online e a procura pelos conteúdos visuais.³⁰¹

Figura 17: Categorias principais do material sexual "auto-gerado" pela criança, e danos associados.



As motivações para a "auto-produção" são variadas e complexas.

Foram definidas três categorias alargadas para este tipo de material "auto-gerado" (ver Figura 17):

- O material não-sexual é conteúdo "autogerado" que não é de cariz sexual, mas que é desviado e usado em conexão com a exploração sexual e o abuso de crianças online.³⁰² Embora as vítimas possam não ter consciência, esse material causa danos principalmente porque facilita a atividade do abusador. Em alguns casos, os danos diretos acontecem quando os abusadores manipulam digitalmente as imagens das vítimas para que pareçam sexuais para, em seguida, as chantagear, ameaçando partilhar as imagens das crianças.³⁰³
- O material "autogerado" de forma voluntária é, normalmente, partilhado entre adolescentes, sejam amigos ou colegas. Esta categoria abrange a "autoprodução" apenas de adolescentes — as crianças mais novas não têm como consentir, logo, uma "autoprodução" que as implique não pode ser considerada "voluntária". Neste cenário, o dano acontece quando as imagens são (re)partilhadas contra a vontade de um jovem. Em 39 estudos diferentes, envolvendo 110.380 participantes com idades entre os 12 e os 17 anos, 12% dos jovens admitiram já ter encaminhado uma imagem sexual "autogerada" sem consentimento.³⁰⁴ O estudo Economist Impact, realizado em conjunto com este relatório, revelou que 29% dos inquiridos relataram ter tido a experiência de alguém ter partilhado imagens e/ou vídeos seus, de cariz sexual e explícito, sem o seu consentimento. Também os destinatários da partilha não-solicitada de material "autoproduzido" voluntariamente, podem sofrer danos na sua integridade emocional ou moral.³⁰⁵
- ' O material "auto-gerado sob coação" envolve o aliciamento e treino das crianças para a criação de imagens sexuais e tem sido associado à prática de "capping" (captação ilícita de imagens).³⁰⁶ As crianças envolvidas em "auto-produção sob coação" podem não se aperceber da situação, podendo até entender as suas próprias ações como voluntárias.

As diferentes rotas para a "autoprodução" criam um desafio para os as equipas de intervenção. Embora o conteúdo das imagens ou vídeos possa corresponder à definição legal de "material de abuso sexual de crianças" e, portanto, invocar certos processos legais uma vez detetados, a intenção por trás da criação ou da partilha das imagens pode não ser clara. É fundamental compreender o contexto de produção e/ou partilha para garantir que a resposta possa ser corretamente ajustada. Ou seja, uma abordagem caso a caso será sempre necessária.

INTERNET WATCH FOUNDATION Material sexual "autogerado" por irmãos

A Internet Watch Foundation (IWF) é uma organização de proteção da criança que usa tecnologia para encontrar e remover da Internet os materiais de abuso sexual infantil.³⁰⁷ Em 2020, a IWF notou um aumento alarmante no volume de material "autogerado" detetado online.³⁰⁸ E neste conjunto, os analistas observaram uma tendência particularmente perturbadora em que os predadores aliciavam as crianças para que envolvessem outras crianças na "autoprodução".

A análise de imagens sexuais "autogeradas" relatadas à IWF entre setembro e dezembro de 2020 revelou:

511

imagens e vídeos envolvendo irmãos

65%

dos casos eram de uma ou ambas as crianças envolvidas em contacto sexual direto uma com a outra

46%

deste material foi classificado como conteúdo de Categoria A, mostrando as formas mais extremas de abuso sexual de crianças.

Em muitos casos, as crianças tinham sido manipuladas ou coagidas por adultos a fazerem sexo ao vivo, sendo que os vídeos e capturas de ecrã resultantes foram partilhados em diversas plataformas online. Alguns dos adultos faziam-se passar por crianças e, por vezes, o abuso assumia a forma de jogo ou "desafio". As crianças envolvidas raramente demonstravam qualquer compreensão da natureza sexual dos atos que estavam a ser obrigadas a praticar.

Embora as evidências sugiram que a partilha de imagens sexuais não seja uma prática pouco frequente entre os jovens (ver Figura 18), algumas crianças têm maior probabilidade de serem pressionadas a fazê-lo, o que as pode colocar em situação de maior risco de coação e/ou partilha não consensual.

HAMOGELO:

A história da Maria

A Maria* tem 15 anos e vive na Grécia. A jovem começou a falar com Yannis*, um rapaz de 20 anos, numa plataforma de encontros. Maria acedeu à plataforma por curiosidade e tédio: as restrições do confinamento por COVID-19 ditaram o afastamento da escola e das normais atividades ao ar livre.

Yannis perguntou-lhe sobre como era a vida dela durante a pandemia, escutou-a e até parecia partilhar dos seus sentimentos. O rapaz falava com ela todos os dias, fazendo com que a proximidade entre ambos crescesse.

Yannis acabou por coagir a Maria a enviar-lhe imagens sexuais "autogeradas" de si mesma, convencendo-a de que seria um passo em frente no "relacionamento" de ambos e que ficaria em segredo entre eles. Com o tempo, Yannis começou a exigir mais, inclusive vídeos.

Maria tentou recusar, mas Yannis ameaçou publicar as suas fotos nas redes sociais. Sentindo-se desesperada, ela procurou ajuda online e encontrou a linha de apoio Helpline da Hamogelo 1056.

A Helpline disponibilizou apoio e aconselhamento anónimos e ajudou a Maria a conversar com os seus pais sobre o problema. A família contactou a linha de apoio em conjunto e o caso foi encaminhado para a Divisão de Crimes Cibernéticos da Polícia grega, o que resultou na posterior detenção de Yannis.

Hamogelo, ou "O Sorriso da Criança", é uma organização grega que apoia crianças vítimas de violência, abuso, extorsão, pobreza e problemas de saúde. Até ao momento, a instituição apoiou mais de 1,7 milhões de crianças e famílias.

*pseudónimos

Um estudo recente revelou que adolescentes belgas flamengos que se identificam como LGBTQ+ foram mais frequentemente pressionados a partilharem imagens sexuais do que os seus pares heterossexuais.³⁰⁹ Um estudo sobre "Adolescentes, Sexting e Riscos" conduzido pela instituição solidária Internet Matters, do Reino Unido, revelou também que os 'grupos vulneráveis' (crianças portadoras de uma ou mais deficiências ou deficiências físicas, mentais ou sociais) são muito mais propensos a serem pressionados ou chantageados para partilhar "nudes".³¹⁰ O assédio sexual na forma de pedidos persistentes de material "autogerado" não é, aparentemente, um fenómeno incomum em alguns países. Um inquérito do UK Office for Standards in Education, Children's Services and Skills (OFSTED), revelou que, de uma amostra de 900 jovens, 80% das raparigas disseram que foram "muito" pressionadas ou pressionadas "por vezes" a partilharem imagens sexuais de si mesmas. Outras possíveis motivações para a "autoprodução" incluem uma história anterior de abuso, o envolvimento em "comportamentos mais arriscados online e no mundo físico" e uso frequente de salas de chat.^{311 312}

De acordo com a IWF, as raparigas no início da adolescência tendem muito mais a aparecer neste tipo de imagens: 95% do conteúdo sexual "autoproduzido" reportado à organização, em 2020, apresentava raparigas com idades entre os 11 e os 13 anos.³¹³ No entanto, outros estudos sugerem que uma proporção equivalente ou até maior de rapazes está também a "autoproduzir" esse tipo de conteúdos:

- Um estudo americano envolvendo 1.000 jovens dos 13 aos 17 anos revelou que a proporção de rapazes que partilharam fotos suas de nudez foi de 1 em 10 (para as raparigas, o número foi de 1 em 5).³¹⁴
- Um questionário online do Reino Unido envolvendo 1.001 jovens dos 13 aos 17 anos identificou um número igual de rapazes e raparigas que tiraram fotos de si mesmos integralmente nus.³¹⁵
- Um inquérito envolvendo 500 jovens dos 13 aos 24 anos que vivem no vale de Katmandu, no Nepal, revelou que 18% dos rapazes e 5,2% das raparigas afirmaram terem-se fotografado a si mesmos nus.³¹⁶

Seria necessária uma investigação mais aprofundada para compreender melhor o papel do género enquanto fator de risco e em que medida tal pode diferir nos diferentes tipos de danos ligados ao material sexual "autogerado" de crianças (por exemplo, produção coagida versus "autoprodução" voluntária). Outros fatores de risco comuns da "autoprodução" estão relacionados com o modo de utilização da Internet pelas crianças. O aumento do uso de dispositivos móveis³¹⁷ limita a possibilidade de supervisão pelos pais. Deste modo, aliado à facilidade de acesso aos conteúdos e às plataformas para adultos (dada a falta de verificações de idade, ou verificações que são prontamente contornadas),³¹⁸ torna-se fácil imaginar de que modo as condições para "autoprodução" se propiciam, mesmo na ausência de outras causas que contribuam para o risco.

A "autogeração" em troca de dinheiro pode vir a aumentar devido à pobreza trazida pela pandemia de COVID-19.

Entende-se "autoprodução" com motivação comercial quando as crianças criam imagens ou vídeos sexuais de si mesmas em troca de retribuição monetária. Os relatos de "autoprodução" com motivação comercial estão a surgir por todo o mundo. Nas Filipinas, as autoridades descobriram casos de adolescentes que criam grupos em plataformas de redes sociais para vender imagens e vídeos sexuais "para financiar as despesas com cursos online". Um desses grupos reunia 7000 membros antes de ser removido.³¹⁹ No Camboja, alguns jovens (a maioria, raparigas) usa o próprio material sexual para vender produtos cosméticos online. Algumas pesquisas realizadas com jovens cambojanos sugerem que esse tipo atividade pode culminar em abuso sexual grave.³²⁰ O NCMEC chamou a atenção para casos de crianças desaparecidas que, mais tarde, se soube que vendiam material sexual autogerado em plataformas de assinantes, sendo que foram encontradas evidências de que existe uma ligação à exploração organizada e ao tráfico.

Independentemente das circunstâncias, todos os atos de "autoprodução" com motivação comercial são quase sempre danosos para a criança, sendo que o material produzido é tendencialmente ilegal. Este problema exige uma resposta urgente e ponderada por parte dos legisladores. O inquérito de 2020 da Netclean às Polícias dos vários países revelou que algumas tinham já notado o aumento na "autoprodução" em troca de dinheiro durante a pandemia, enquanto outras antecipavam a continuação da tendência à medida que as condições económicas se deterioraram, e as crianças veem esta atividade como uma forma de "ganhar dinheiro para coisas que, de outra forma, não poderiam pagar".³²²

Os danos provocados por material "autogerado" abrange o assédio, a partilha repetida e a culpabilização da vítima.

A IWF encontrou casos em que os abusadores que visualizam o conteúdo "autogerado" tentam identificar e localizar a(s) vítima(s), com a intenção de a(s) coagir a gerar mais e mais conteúdo.³²³ Em outros cenários, o(s) autor(es) inicial(is) é alguém conhecido, tal como sucede com o "abuso presencial", sendo, muitas vezes, "pessoas em quem as crianças confiam e das quais dependem".³²⁴ Ambos os fatores podem gerar uma sensação de inevitabilidade em torno do abuso, que é amplificada pela partilha repetida. Em 2014, a IWF avaliou mais de 3800 imagens e vídeos sexuais "autogerados" e revelou que 90% tinham sido "obtidos no local do upload original mas estavam a ser redistribuídos em sites terceiros".³²⁵

Os danos infligidos pela "autogeração de material" tende a ser grandemente exacerbado pela tendência de culpar a vítima. De acordo com uma pesquisa da Thorn, 60% das crianças culpam a vítima quando o material "autogerado" é partilhado mais adiante, enquanto que 55% dos cuidadores acreditam que a vítima é, em grande parte ou totalmente, responsável pela partilha repetida.³²⁶ Tais atitudes prejudicam a exposição e as denúncias, e alimentam estigmas que impedem as crianças de avançarem e pedirem ajuda.

As iniciativas de denúncia e as soluções de tecnologia podem conter a proliferação do material "autogerado", mas a prevenção exige uma abordagem mais multifacetada.

A campanha "Report Remove" foi lançada, no Reino Unido, em 2020, para permitir que as crianças relatassem anonimamente materiais "autogerados" e solicitassem sua remoção.³²⁷ Estas iniciativas reduzem os obstáculos à exposição do problema. Os controlos ao nível do dispositivo que evitam que as crianças captem imagens e vídeos sexuais podem igualmente oferecer um "tempo de pausa" eficaz para conter o aumento da "autoprodução". Um exemplo disto é o detetor de ameaças de imagem e vídeo "SafeToWatch" (ver o estudo de caso anexo). Essas soluções têm implicações para o direito das crianças à privacidade, que precisará ser cuidadosamente considerado no sentido de apoiar a sua mais ampla adoção e implementação.

Uma prevenção sustentável a longo prazo exigirá abordagens refletidas e baseadas nas experiências complexas das crianças e dos jovens que se debatem com o processo de autodescoberta pessoal nesta era digital. Uma vez que a partilha de imagens sexuais "autoproduzidas" não é pouco frequente e que nem sempre causa danos, o foco excessivo nas potenciais consequências negativas corre o risco de "gerar conselhos que serão rejeitados por não corresponderem às experiências reais dos jovens".³²⁸ A educação será a chave para proteger as crianças de se tornarem vítimas de coação e das potenciais consequências negativas da "autoprodução voluntária". As iniciativas educativas podem também ajudar a promover o desenvolvimento sexual saudável e a compreensão do consentimento.³²⁹ Um exemplo de uma dessas iniciativas é a campanha "Send me a pic" do NCA, que visa promover um diálogo construtivo com os jovens em torno da partilha de imagens de nudez.

SAFETONET:

SafeToWatchSafeToNet é uma empresa de tecnologia de segurança que implementa soluções de inteligência artificial e análise comportamental para ajudar a manter as crianças seguras online. A SafeToNet acredita que as funcionalidades de design de segurança para crianças devem ser integrados nas tecnologias ao nível do dispositivo e do sistema operativo.

A inovação mais recente da SafeToNet é o SafeToWatch, um detetor de ameaças para fotografias e vídeo que pode interromper a criação de material de abuso sexual infantil, em tempo real e na fonte. Este recurso utiliza tipos de inputs, como o áudio e o vídeo, para avaliar o ambiente digital da criança, aplicando um conjunto de algoritmos exclusivos para permitir a deteção em tempo real de material de abuso sexual infantil. O SafeToWatch funciona da mesma maneira, independentemente de o conteúdo ser transmitido ao vivo por terceiros ou "autogerado" pelas próprias crianças. A deteção de tais imagens aciona imediatamente a restrição das câmaras e dos microfones, o que pode bloquear o funcionamento de uma aplicação ou de todo o dispositivo móvel, impedindo, assim, que a foto ou o vídeo seja efetuado. As imagens não são retidas, garantindo o direito das crianças à privacidade. Ao contrário das ferramentas de deteção ao nível da plataforma, esta tecnologia pode ser implementada prontamente em ambientes encriptados end-to-end. Fundamental para o sucesso futuro do SafeToWatch e inovações semelhantes é o acesso fiável aos dados do governo e da polícia para treinar os algoritmos e otimizar a eficácia deste tipo de soluções.

A SafeToNet adquiriu 77 lojas de telemóveis na Alemanha, para levar a segurança cibernética para o comércio de rua.³³⁰

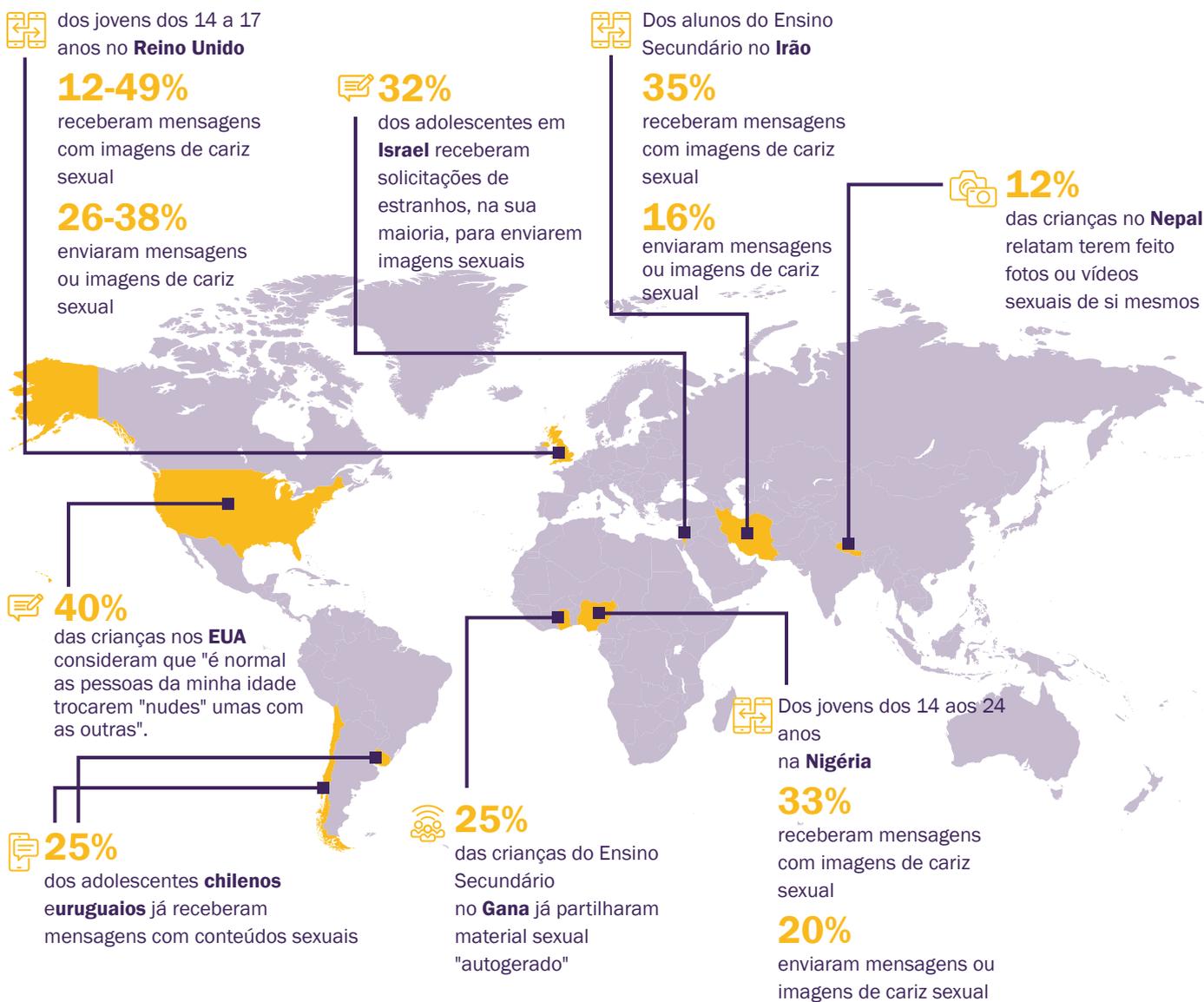
Em alguns países, as alterações à legislação permitiriam dar uma resposta mais eficaz, e mais focada nas crianças, relativamente à questão do material sexual voluntariamente "autoproduzido".

Algumas estruturas legais exigem uma reforma urgente para evitar a criminalização continuada das crianças por comportamentos que são indiscutivelmente "parte integrante da descoberta normal da própria sexualidade".³³¹

Dentro desta linha, algumas regiões da Austrália descriminalizaram o "sexting" entre pares, ou seja, amigos e colegas.³³² Este tipo de abordagem é possível nos termos da Convenção de Lanzarote, que inclui uma "isenção" da criminalização do abuso sexual infantil entre crianças se determinados critérios forem cumpridos. Esta orientação pode ajudar os países a definirem respostas mais adequadas para crianças e adolescentes envolvidos na geração, visualização ou partilha de conteúdo "autogerado".³³³ No Reino Unido, o número de jovens que entram no sistema de justiça criminal em resultado de "autogeração" de material sexual duplicou entre 2007 e 2016.³³⁴ Recentemente, o governo aconselhou os profissionais da educação a que as "crianças e jovens não fossem criminalizadas por partilharem fotos de nudez e semi-nudez".³³⁵

Contudo, alguns jovens ultrapassam, de facto, a linha daquilo que já é considerado um comportamento sexual danoso e ofensivo. Conforme salientado pela UNICEF, "os pares constituem uma proporção significativa dos responsáveis por atos de abuso sexual contra outras crianças e adolescentes".³³⁶ Esses cenários expõem a lacuna existente na resposta uma vez que "os modelos de intervenção foram previstos, na sua maioria, para criminosos adultos".³³⁷ Manifestando-se, em muitos casos, como um dano causado pelos seus pares, a questão do material sexual "autogerado" demonstra a importância de estratégias capazes de gerar respostas que atendem às necessidades das crianças que tanto sofrem abusos como se envolvem em comportamentos sexuais danosos em relação a seus pares.³³⁸

Figura 18: Quão comum é a partilha de imagens e mensagens de teor sexual entre jovens? 339 340 341 342 343 344 345 346



06 Danos

Streaming ao vivo de situações de exploração e abuso sexual de crianças

O streaming ao vivo está em ascensão, facilitado pela conectividade e pela disponibilidade de dispositivos de transmissão de imagem e som de baixo custo.

O streaming ao vivo pode envolver o abuso presencial de uma ou mais crianças, sendo transmitido online, ou uma criança(s) a ser(em) forçada(s) a "praticar" atos sexuais em frente a uma webcam — geralmente em troca de compensação monetária.

A prática do streaming ao vivo está em ascensão, facilitada pela alta conectividade e a pela disponibilidade de dispositivos de transmissão de imagem de baixo custo. Manifesta-se, muitas vezes, como um crime transfronteiriço que exige uma resposta internacional coordenada.

Ao contrário do streaming ao vivo "autogerado" (ver capítulo Dano: *Material Sexual Infantil "autogerado"*), este tipo de abuso é geralmente facilitado por terceiros. Embora haja casos em que a vítima e os seus abusadores estão na mesma localidade, a maioria dos crimes ultrapassa as fronteiras nacionais. Conforme explicado pela ECPAT, este tipo de abuso "tende a aproveitar-se da disparidade económica, em que perpetradores de países desenvolvidos acedem a vítimas em países em vias de desenvolvimento".³⁴⁷ A questão exemplifica o dano generalizado causado pelas desigualdades globais num mundo conectado.

De acordo com a Interpol, o streaming ao vivo pago está em crescimento.³⁴⁸ As evidências sugerem que essa tendência está a ser exacerbada pela pandemia. Nas Filipinas, país descrito pela UNICEF como sendo o "epicentro global do comércio de abuso sexual ao vivo",³⁴⁹

foi observado um aumento de 265% dos casos durante o período de quarentena de março a maio de 2020. A organização Save the Children estabeleceu um paralelo com o agravamento da pobreza, sugerindo que difíceis condições económicas resultantes da COVID-19 estão a fazer com que mais indivíduos se envolvam em esquemas de streaming ao vivo para ganhar dinheiro.³⁵⁰

A atividade de streaming ao vivo pode implicar a prática de uma série de crimes. A maioria das vítimas identificadas encontra-se no Hemisfério Sul, mas o abuso acontece em muitas regiões do globo.

No contexto das transmissões ao vivo, os abusadores implicam os indivíduos que organizam a exploração assim como aqueles que direcionam e "consomem" o conteúdo. Os indivíduos que organizam o abuso podem pertencer a grupos criminosos organizados, mas também podem fazer parte do círculo de confiança da vítima. Através da análise de casos de streaming ao vivo realizada nas Filipinas, o IJM relatou que a maioria dos infratores (69%) eram as mulheres da família com motivação financeira ou pessoas próximas das vítimas.³⁵¹ O facto dos "facilitadores" de streaming ao vivo serem motivados principalmente por questões financeiras, permite distinguir este crime das muitas outras formas de abuso sexual de crianças.

Os dados disponíveis indicam que os indivíduos que "consomem" o abuso por transmissão ao vivo são predominantemente da Europa, América do Norte e Austrália.³⁵² Esses criminosos procuram o abuso por streaming ao vivo, visando as regiões do mundo "com elevados níveis de pobreza, com mecanismos domésticos de proteção infantil limitados, e fácil acesso às crianças".³⁵³ A acusação dos chamados infratores do "lado da procura" tende a concentrar-se no crime de visualização de material de abuso sexual infantil, claramente subestimando a sua participação global no crime. Conforme explica o IJM, existe justificação para processar esses indivíduos enquanto traficantes, uma vez que "abusam de seu poderio financeiro" ao "oferecer" pagamento pelos atos de exploração, indo encaixar, dessa forma, na definição internacionalmente aceite de tráfico humano, conforme o estabelecido no Protocolo de Palermo.³⁵⁴

A maioria das vítimas de streaming ao vivo identificadas reside no sudeste da Ásia, em particular nas Filipinas,³⁵⁵ mas também existem vítimas em regiões como Europa, Rússia e EUA.³⁵⁶ Isto faz ressaltar a importância de evitar a tipificação estreita do streaming ao vivo como um crime que afeta apenas crianças e jovens em países pobres.³⁵⁷ Para além de causar grande trauma e sofrimento nas vítimas, de acordo com um estudo de casos do Sudeste Asiático, o streaming ao vivo pode traduzir-se num "primeiro passo para as crianças entrarem na exploração sexual com motivação comercial "offline".³⁵⁸

INTERNATIONAL JUSTICE MISSION:

A história de Ruby

Aos 16 anos, Ruby* viu-se privada da sua liberdade e forçada a fazer tudo aquilo que os seus abusadores online exigissem enquanto dirigiam a transmissão ao vivo para a Internet do abuso sexual a que a jovem estava a ser submetida.

A provação de Ruby começou quando um traficante a contactou por mensagem privada numa rede social e conquistou a sua confiança com uma oferta de emprego numa loja de informática, com alojamento e alimentação incluídas na função. O traficante e um cúmplice ofereceram-se ainda para cobrir as despesas de viagem de Ruby quando esta viesse ao seu encontro. Ruby não demorou a descobrir que o trabalho não correspondia ao prometido. Ela quis vir-se embora, mas não o poderia fazer até que saldasse aquilo em que se converteu sua "dívida" de viagem, o que se tornou quase impossível devido ao seu vencimento ser absorvido pelos artigos caríssimos que o traficante a obrigava a comprar.

A certa altura, a jovem tentou escapar, mas foi ameaçada com uma faca. Ruby descreve o abuso pelas suas próprias palavras:

"Era paga por cada programa nojento que fazia em frente à câmara do computador com o cliente. E durante o período em que fazia todos aqueles programas nojentos, sinto que perdi toda a minha autoestima ao ponto de ficar com nojo de mim mesma, também.

Foi como estar presa num quarto completamente escuro, sem a mínima nesga de luz. Viver deixa de fazer sentido.

Fazes programas nojentos todos os dias, várias vezes, e no final, vais dormir e repetes a mesma rotina no dia seguinte, como se não houvesse fim."

O IJM apoiou as autoridades filipinas para atuarem de acordo com uma pista da US Homeland Security Investigations (HSI) para localizar Ruby e proceder ao seu resgate, dela e de outras cinco jovens. O casal que comandava a operação de tráfico foi posteriormente condenado e sentenciado. O IJM prestou assistência a Ruby non seu percurso rumo à recuperação, que Rubi descreveu da seguinte forma: "Não foi nada fácil. Levei anos, anos, para me recuperar das experiências dolorosas, das experiências traumáticas. Sabes, à noite, quando alguém apaga a luz de repente, eu salto da cama porque simplesmente não consigo dormir sem a luz acesa porque passei a ter muito medo do escuro. Foi assim que fiquei durante anos."

Hoje, Ruby é livre e sente-se segura. Está a ponderar formar-se em Direito na esperança de ajudar outras raparigas encurraladas em circunstâncias semelhantes.

A International Justice Mission é uma ONG que estabelece parcerias com os sistemas de justiça locais de todo o mundo para acabar com a violência contra as pessoas que vivem na pobreza. Através do seu Center to End Online Sexual Exploitation of Children, a instituição reforça os sistemas de proteção das crianças contra a produção e streaming de material de abuso sexual infantil.

*Um pseudónimo

O facto de os limites serem cada vez mais ténues entre a prática de streaming ao vivo e o tráfico humano complica, de forma crescente, as investigações sobre o streaming a vivo.

A nível mundial, um terço das vítimas de tráfico detetadas são crianças. Destas, 72% das raparigas e 23% dos rapazes são traficados para fins de exploração sexual.³⁵⁹ O tráfico de crianças envolve frequentemente formas de abuso online e tem sido associado ao aumento do volume de material disponível de abuso sexual de crianças. O Gabinete das Nações Unidas para as Drogas e o Crime (UNODC) destaca o caso de traficantes, na Tailândia, que "exploram sexualmente um grande número de crianças e produzem várias centenas de milhares de imagens para distribuição online".³⁶⁰

A ligação entre o streaming ao vivo e o tráfico tende a tornar-se cada vez mais estreita à medida que mais traficantes alteram os seus modelos de negócio online para contornar o impacto das restrições da COVID-19.³⁶¹ Conforme salientado no Relatório de Tráfico Global do UNODC de 2021, o benefício das tecnologias da Internet para os traficantes é significativo, em especial porque "facilitam os atos de exploração perante um público maior do que seria normalmente possível com o tráfico tradicional."³⁶² As evidências sugerem que o streaming ao vivo aumentou a sua popularidade durante a pandemia enquanto alternativa ao

abuso sexual infantil presencial.³⁶³ Seguramente, os traficantes online estarão bem posicionados para tirar proveito da crescente procura de "serviços remotos".

Quando o streaming ao vivo se apresenta como parte do tráfico de crianças, pode criar especiais dificuldades que complicam as investigações. Nas Filipinas, a UNICEF concluiu que os casos de tráfico com exploração online "são confundidos com casos de crimes cibernéticos" — um problema capaz de provocar atrasos na referênciação.³⁶⁴ As vítimas de tráfico humano tornam-se também mais difíceis de identificar, precisamente devido à contaminação com outras formas de abuso.³⁶⁵

Globalmente, um terço das vítimas de tráfico detetadas são crianças. Destas,

72% E **23%**
DAS RAPARIGAS DOS RAPAZES

são traficados para fins de exploração sexual.

É necessária uma colaboração mais proativa entre as Polícias e os prestadores de serviços financeiros e online de modo a melhorar a detecção de abusos transmitidos por streaming ao vivo.

É tecnicamente possível interromper a prática do streaming ao vivo. Conforme descrito no capítulo Danos: *Partilha e/ou armazenamento de material de abuso sexual infantil*, existem classificadores para detetar material de abuso sexual de crianças. No entanto, a maioria dos abusos transmitidos ao vivo acontecem online, em "conversas" privadas e, portanto, não estão sujeitos à triagem ou revisão do moderador. A menos que um infrator faça uma gravação, a transmissão não deixa geralmente rastro. A falta de provas torna difícil, por isso, processar este tipo de crimes — uma dificuldade agravada pela ausência de disposições na legislação atual que criminalize a prática.³⁶⁶ Os "consumidores" de abusos transmitidos ao vivo demonstram geralmente uma baixa sofisticação técnica (a maioria dos streamings ao vivo ocorre na web de superfície),³⁶⁷ possivelmente porque percebem que as probabilidades de serem detetados e condenados são baixas.

A monitorização de conversas privadas para detetar streamings ao vivo pode ser considerada por alguns utilizadores da Internet como uma invasão de privacidade justificável. Mas ainda que estes mecanismos fossem aceites e implementados por alguns prestadores de serviços online, os infratores poderiam facilmente migrar para qualquer outra plataforma E2EE, que são cada vez mais numerosas. Este recurso oculta o conteúdo das comunicações, tornando impossível a detecção de streams e, portanto, evidenciando a necessidade urgente de diversificar os métodos de interrupção.

Os indicadores financeiros são citados por muitos como as "pistas" mais eficazes para ajudar na identificação de abuso sexual por streaming ao vivo. Existe já uma tradição de colaboração bem-sucedida com o setor financeiro. Uma iniciativa direcionada em 2017 alcançou a eliminação virtual do uso de cartões de crédito nos EUA para a compra de conteúdo de abuso sexual de crianças online.³⁶⁸ O Australian Transaction Reports and Analysis Centre alavancou com sucesso a sua parceria público-privada, a Fintel Alliance, para bloquear transações ligadas à exploração infantil.³⁶⁹

Muitas agências policiais e prestadores de serviços financeiros já estabelecem colaborações na investigação de crimes relacionados com o streaming ao vivo. No entanto, existe potencial para uma abordagem mais proativa. Tal como explica o IJM, enquanto que as empresas "normalmente cedem" quando as autoridades policiais solicitam informações, é mais importante "que elas identifiquem, reportem e interrompam de forma proativa (...) as transferências de dinheiro em tempo real".³⁷⁰ O potencial para tal colaboração estreita pode ser complicado pela contínua diversificação dos serviços financeiros. O uso mais alargado de criptomoedas é outra fonte de dificuldades, pois embora seja possível rastrear os pagamentos, nem todas as agências policiais têm o know-how para o fazer.³⁷¹

Em 2020, o Grupo Egmont (um consórcio de unidades globais de inteligência financeira) realizou um estudo sobre as possíveis utilizações da inteligência financeira para combater os streamings abusivos. O estudo destacou vários desafios. Um deles, por exemplo, é a dificuldade de distinguir as transações de streaming ao vivo que correspondam ao pagamento por conteúdo sexual adulto, a atividades fraudulentas ou a outros crimes. No geral, concluiu que existem benefícios em "combinar informações financeiras" com outras fontes, através da troca de dados com autoridades policiais e entidades do setor privado.³⁷² As conclusões do projeto demonstram a importância de uma abordagem coordenada e multi-setorial para enfrentar com eficácia o abuso transmitido por streaming ao vivo. Com as estruturas apropriadas em vigor para permitir a partilha legal de dados, as informações de prestadores de serviços online podem fornecer um complemento poderoso para a inteligência financeira, ao evidenciarem, por exemplo, os "sinais" (metadados e indicadores comportamentais) que apontem para uma provável atividade nefasta dos utilizadores.

Uma prevenção sustentável das práticas nocivas por streaming ao vivo requer formação e atribuição de poderes à comunidade, a capacitação da polícia e maior consistência na abordagem a nível mundial.

A UNICEF realizou uma análise dos casos de abuso sexual de crianças online nas Filipinas, tendo verificado que o livestreaming é, em muitos casos, facilitado pela família ou dentro da comunidade da vítima e "justificado" por certas crenças culturais. Por exemplo, a ideia de que o dano não é causado se a criança não for tocada, ou a noção de que as crianças devem ajudar as famílias financeiramente.³⁷³ Este contexto dificulta a proteção (já que as crianças em tais circunstâncias podem nem mesmo reconhecer o abuso) e coloca uma pressão maior sobre as agências de proteção da criança, normalmente já sobrecarregadas, na identificação das crianças em risco. A formação e a atribuição de poderes à comunidade são essenciais para efetivar a prevenção sustentável do livestreaming abusivo, para aumentar a consciencialização sobre os danos causados por este tipo de abuso, para erradicar as crenças prejudiciais e para promover práticas de proteção. São também vitais as iniciativas que dão voz às crianças, para assegurar que estas tenham meios para se pronunciarem e procurarem ajuda.

Atualmente, não existe uma definição internacionalmente aceite para o crime de exploração e abuso sexual de crianças durante o livestreaming. Embora em muitos países tal se enquadre nas disposições existentes relacionadas com a exploração sexual infantil,³⁷⁴ isso criaria uma barreira à colaboração policial internacional, restringindo a capacidade de desenvolver abordagens de investigação consistentes. Significa igualmente que os infratores poderiam escapar à punição com base na cláusula de "dupla incriminação", que estabelece que a conduta deve ser criminalizada tanto no país de origem do abusador como no país onde ocorreu o crime.³⁷⁵

Em alguns países, as limitações da investigação acabam por diminuir o risco de deteção e punição. Por exemplo, na Austrália, 90% dos processos de livestreaming bem-sucedidos dependem do uso de táticas secretas. Em contraste, no Camboja, as investigações secretas não são permitidas por lei.³⁷⁶ No México, os esforços para combater o crime são comprometidos pela falta de conhecimento especializado por parte dos legisladores, o que impede a consideração integral dos métodos de deteção e de investigação.³⁷⁷

Atualmente, não existe uma definição internacionalmente acordada para o crime de transmissão online de abuso e exploração sexual de crianças ao vivo.

Recomendações

A Avaliação da Ameaça Global deste ano demonstra que a escala de exploração e abuso sexual de crianças online continua em crescimento.

As recomendações infra permitiriam que os governos, a sociedade civil, as comunidades e os prestadores de serviços online capitalizassem os desenvolvimentos positivos para melhorar a resposta às ameaças, e também no tocante à prevenção. Estas recomendações estão alinhadas com o âmbito da Resposta Estratégica Global da WeProtect Global Alliance.³⁷⁸

A exploração sexual e o abuso infantil online são questões de relevância mundial que exigem um esforço de colaboração internacional contínua e um diálogo intersetorial.

A Aliança atende a essa necessidade facilitando o contacto e a interajuda entre os governos, o setor privado e a sociedade civil — gerando compromisso político e abordagens práticas que tornem o mundo digital seguro para as crianças. Para saber

mais visite: www.weprotect.org

Tema	Recomendação
Financiamento	Os governos, o setor privado e a sociedade civil devem investir fundos suficientes para enfrentar a ameaça da exploração e do abuso sexual de crianças online. Os atuais níveis de investimento não são proporcionais à escala e alcance do problema, nem sequer suficientes para permitir a subida de etapa necessária para dar resposta à ameaça global. ³⁷⁹
Políticas/Legislação	<p>Os governos deverão criar leis que criminalizem todos os crimes relacionados com a exploração e o abuso sexual de crianças online, com base em quadros de atuação acordados internacionalmente, mas que, simultaneamente, evitem a criminalização das próprias crianças.</p> <p>Os governos deverão investir no reforço dos sistemas de proteção infantil no sentido de prevenir e responder à exploração sexual e abuso de crianças em todos os contextos.</p> <p>Os governos deverão ponderar as opções legislativas que reforcem a resposta aos crimes de exploração e abuso sexual de crianças online. As leis deverão estabelecer padrões para as denúncias apresentadas pela indústria digital, a remoção rápida dos materiais de abuso sexual infantil, estabelecer uma base para a utilização legal e transparente de ferramentas de deteção de material de abuso sexual de crianças online. O alinhamento internacional deverá ser procurado para aumentar a colaboração global no combate à ameaça.</p>

<p>Justiça Criminal</p>	<p>Os governos deverão investir na dissuasão e na reabilitação de forma a ajudarem as pessoas em risco de cometer crimes ou os criminosos a alterarem ou a gerirem o seu comportamento. Os governos devem financiar unidades especializadas de policiamento para cultivar e manter a especialização na resposta às ameaças, e assim melhorar os resultados das investigações internas de cada país. Os governos deverão também investir na criação e reforço das capacidades de policiamento internacional, reforçando a colaboração no tratamento dos crimes transfronteiriços e tecnologicamente sofisticados.</p> <p>Os governos e as agências de policiamento deverão consultar as respetivas congéneres internacionais no sentido de desenvolverem abordagens consistentes na investigação dos crimes transfronteiriços e solucionar os desafios comuns à investigação como, por exemplo, a recolha de provas dispersas por diferentes jurisdições.</p>
<p>Serviços de apoio e capacitação da vítima</p>	<p>Para reduzir o trauma da vitimização repetida, os legisladores deverão trabalhar com a indústria para definir procedimentos-padrão para a remoção atempada, da Internet, do material de abuso sexual de crianças, bem como para reduzir a reincidência das imagens e criar mecanismos de denúncia à medida das necessidades das crianças, independentemente dos processos da Justiça Criminal. Os governos deverão investir em iniciativas de apoio e capacitação das vítimas ao nível dos serviços de proteção à criança, de modo a garantir que os funcionários sejam formados em abordagens ajustadas ao tipo de traumas, ou seja, em como apoiar vítimas de abuso online e a crianças de grupos marginalizados.</p> <p>Todas as partes interessadas deverão ponderar a interação segura e apropriada com as crianças sobreviventes de abuso sexual como base para a criação e avaliação de serviços, políticas e modalidades de apoio eficazes.</p>
<p>Tecnologia</p>	<p>Os prestadores de serviços online deverão adotar uma abordagem de "Safety by Design" que inclua a avaliação do impacto de todos os produtos e serviços na perspectiva dos direitos da criança.</p> <p>Os prestadores de serviços online deverão identificar e, conforme adequado, alertar, expulsar e reportar os agentes que representem um risco para as crianças. Os prestadores de serviços online deverão publicar relatórios de transparência regulares, detalhando as ações empreendidas para reduzir o risco online para as crianças, bem como os mecanismos utilizados para monitorizar a sua eficácia.</p> <p>Os programadores de tecnologias digitais de segurança online deverão continuar a trabalhar na melhoria da precisão das ferramentas de estimativa de idade, classificadores de deteção de conteúdo desconhecido de abuso sexual infantil (incluindo conteúdo transmitido ao vivo) e em outras soluções de deteção de abuso sexual de crianças online em ambientes encriptados. O código aberto (com controlos apropriados em vigor) deve ser usado para encorajar a colaboração entre os intervenientes relevantes e ajudar a definir critérios consistentes para as tecnologias de segurança.</p>
<p>Social</p>	<p>Os governos deverão integrar o tema da segurança online nos currículos escolares, como complemento a programas mais amplos que abrangem, por exemplo, comportamentos sexuais saudáveis e nocivos.</p> <p>Todas as partes interessadas envolvidas na resposta – incluindo pais, responsáveis e organizações da sociedade civil – devem educar as comunidades sobre o risco e o impacto do abuso sexual sobre as crianças e o que pode ser feito para o prevenir e evitar.</p>
<p>Pesquisa e insight</p>	<p>Governos, organizações da sociedade civil e prestadores de serviços online deverão investir em investigações para:</p> <ul style="list-style-type: none"> • Compreender melhor os caminhos que conduzem ao crime e, de forma associada, a eficácia dos programas de dissuasão, de autoajuda e de gestão dos abusadores. • Compreender melhor as motivações subjacente ao aumento do material sexual "autogerado" por crianças, assim como as características do desenvolvimento social e sexual dos adolescentes. • Compreender os fatores de risco e de proteção que podem agravar ou reduzir o risco de uma criança ser vitimizada, incluindo aqueles que são específicos dos grupos marginalizados da sociedade. • Compreender melhor até que ponto as crianças, em todo o mundo, estão a deparar-se com exploração e abuso sexual infantil facilitada pela tecnologia. • Evidenciar de que modo a ameaça se está a manifestar os países do Hemisfério Sul (já que o quadro das evidências está atualmente mais aprofundado no respeitante ao Hemisfério Norte).

Agradecimentos

AWeProtect Global Alliance gostaria de agradecer às seguintes pessoas e organizações e pelo seu apoio no desenvolvimento da Avaliação da Ameaça Global 2021:

COMITÉ ORIENTADOR

Signy Arnason

Canadian Centre for Child Protection

Rinchen Chopel

South Asia Initiative to End Violence Against Children

Sean Coughlan

Human Dignity Foundation

Toby Dagg

INHOPE/Office of the e-Safety Commissioner

Deborah Denis e Donald Findlater

Lucy Faithfull Foundation

Edward Dixon

Rigr AI

Nicole Epps

World Childhood Foundation

Alexandra Evans

TikTok

Guillermo Galarza

International Centre for Missing and Exploited Children

Alexandra Gelber

US Department of Justice

Susie Hargreaves

Internet Watch Foundation

Afroz Kaviani Johnson

UNICEF

Almudena Lara

Google

Daniela Ligiero

Together for Girls

Remy Malan

Roblox

David Miles

Facebook

Uri Sadeh

Interpol

Michael C. Seto

University of Ottawa Institute of Mental Health Research at the Royal

John Starr e Melissa Stroebel

Thorn

Nena Thundu

African Union

*Agradecimento especial aos Membros da **WeProtect Global Alliance Board** e também à **Getty Images**.*



OUTROS CONTRIBUTOS

Apple	National Centre for Missing and Exploited Children (US)
Arpan	National Crime Agency (UK)
Australian Centre to Counter Child Exploitation	Netsweeper
Australian Department of Home Affairs	Palantir
Australian Federal Police	Policing Institute for the Eastern Region (UK)
Camera Forensics	Project VIC International
ChildSafeNet	SafeToNet
Child Rescue Coalition	SafeBAE
Crisp	Scotiabank
DLT Risk Ltd.	Sentropy
Ethel Quayle	Stuart Allardyce
Europol	Suojellaan Lapsia Ry
Global Partnership to End Violence Against Children (End Violence Partnership)	Terre des Hommes
Dr. Hany Farid	The Technology Coalition
Hamogelo	UK Home Office
International Justice Mission	UK Department for Digital, Culture, Media and Sport
LOCATE	Videntifier
Marie Collins Foundation	Walk Free
Microsoft	YOTI
	ZiuZ Forensic BV

O apoio dado ao desenvolvimento do relatório — enquanto membro do Comité Diretivo ou como Contribuinte — não implica a aprovação (parcial ou total) do conteúdo deste relatório. Este relatório é produto da investigação e redação de Chloe Setter, Natalia Greene, Nick Newman e Jack Perry.

Glossário de Termos

Termo	Definição
Abuso sexual de crianças	O envolvimento de uma criança (qualquer pessoa com menos de 18 anos de idade) numa atividade sexual que ela não compreenda totalmente, seja incapaz de dar o seu consentimento informado ou para a qual a criança não esteja preparada em termos do seu desenvolvimento humano pelo que não tem condições para dar consentimento. ³⁸⁰ Esta é a definição de abuso sexual de crianças adotado pela WeProtect Global Alliance ('a Aliança'), com base nas diretrizes da Organização Mundial da Saúde (OMS).
Exploração sexual de crianças	Forma de abuso sexual infantil que envolve qualquer abuso real ou tentativa de abuso da posição de vulnerabilidade da criança, da posição de poder diferencial ou de confiança. Implica, nomeadamente, lucrar monetariamente, socialmente ou politicamente com a exploração sexual de outra pessoa. ³⁸¹ Pode ser perpetrado por pessoas singulares ou grupos de criminosos. O que distingue a exploração sexual infantil do abuso sexual de crianças é a noção subjacente da troca presente na exploração. ³⁸² Existe uma forte sobreposição entre os dois conceitos, sendo que a exploração é frequentemente uma característica do abuso, e vice-versa. ³⁸³
Exploração e abuso sexual de crianças online	Trata-se da exploração e abuso sexual de crianças online que seja em parte ou integralmente facilitada pela tecnologia, isto é, a Internet ou outro tipo de comunicações sem fios. Este conceito também é conhecido como Exploração e Abuso Sexual de Crianças Online (OCSEA) e exploração e abuso sexual infantil "facilitado pela tecnologia".
Material conhecido de abuso sexual de crianças (CSAM)	Trata-se de qualquer conteúdo visual ou de áudio de natureza sexual envolvendo uma pessoa menor de 18 anos, ³⁸⁴ quer seja real ou não. Nota sobre terminologia alternativa: Algumas organizações fazem a distinção entre material de abuso sexual de crianças e material de exploração sexual de crianças (por exemplo, o Interagency Working Group on the Sexual Exploitation of Children define "material de exploração sexual de crianças" como uma categoria mais ampla que abrange quer o "material que retrata abuso sexual infantil" quer "outro conteúdo sexualizado que retrate crianças"). "Pornografia infantil" é um também um termo alternativo utilizado por algumas organizações. A posição declarada da Aliança é abster-se de usar este termo: "Material de abuso sexual de crianças" considera-se que reflete de forma mais precisa a natureza hedionda da violência sexual contra crianças e é mais adequado para proteger a dignidade das vítimas. Algum material sexual "autogerado" constituiria igualmente material de abuso sexual infantil, dependendo das circunstâncias da sua produção (ver Material sexual infantil "autogerado").



Termo	Definição
Material conhecido de abuso sexual de crianças	Material de abuso sexual de crianças que tenha sido previamente detetado e classificado pelas autoridades policiais e/ou moderadores.
Material de abuso sexual de crianças de "primeira geração"	Material de abuso sexual de crianças que não tenha sido previamente detetado e classificado pelas autoridades policiais e/ou moderadores.
Material de abuso sexual de crianças não fotográfico	Refere-se a caricaturas de imagens geradas por computador ou desenhos que retratam graficamente crianças de forma sexualmente abusiva. ^{385 386}
Material sexualizado de crianças	<p>Material que não representa o abuso sexual de uma criança, mas que é usado para fins sexuais — um exemplo disto pode ser um vídeo de crianças a fazer ginástica, mas que é visto de forma inadequada para satisfação sexual.</p> <p>A sexualização nem sempre é um critério objetivo, e o elemento crucial para julgar tal situação é a intenção de uma pessoa sexualizar uma criança numa imagem ou fazer uso de uma imagem para fins sexuais.</p>
Produção de materiais de abuso sexual de crianças	Criação de material de abuso sexual de crianças presencialmente através fotografia/vídeo/registo áudio, criação de conteúdo textual ou não fotográfico (ou seja, gerado por computador), ou manipulação de material visual já existente de abuso sexual de crianças para criar imagens novas.
Pesquisa por e/ou visualização de material de exploração e abuso sexual de crianças	Pesquisa por material de abuso sexual de crianças na Internet e visualização ou tentativa de visualização do mesmo.
Partilha e/ou retenção de material de abuso sexual de crianças	Download, partilha e/ou retenção de material de abuso sexual de crianças

Termo	Definição
<p>Aliciamento online de crianças com vista à sua exploração e abuso sexual</p>	<p>Quando uma pessoa constrói uma relação de confiança e conexão emocional com uma criança ou jovem com o intuito de a manipular, explorar e abusar sexualmente (de forma facilitada, parcial ou totalmente, pela Internet ou outras comunicações sem fios).³⁸⁸ Nem sempre existe a intenção do encontro presencial.</p> <p>Nota sobre Terminologia Alternativa: algumas organizações usam o termo "preparação online" (conforme definido pelo NCMEC³⁸⁹) quando se referem a este tipo de conceito.</p>
<p>Material sexual "autogerado" pela criança</p>	<p>Conteúdo de natureza sexual, incluindo imagens e vídeos de nudez total ou parcial, produzidos pelas próprias crianças. O material sexual "autogerado" por crianças não constitui um dano por si mesmo (pode ser produzido voluntariamente e partilhado como parte de uma troca adequada para a idade e o estágio de desenvolvimento, nomeadamente entre adolescentes), no entanto, existem situações em que o dano é causado, em primeiro lugar:</p> <ul style="list-style-type: none"> • Quando uma criança ou adolescente é coagida a produzir material sexual "autogerado". • Quando o material sexual "autogerado" voluntariamente é partilhado contra a vontade do adolescente. <p>O presente relatório foca-se na análise das características e limites da "autoprodução" nociva. Esta frase aparece entre aspas ao longo do relatório para evitar qualquer implicação de vontade por parte da criança ou jovem envolvido. Embora o conteúdo possa ir de encontro à definição de material de abuso sexual de crianças, geralmente a intenção não está claramente estabelecida, não podendo, como tal ser assumida em qualquer circunstância.</p>
<p>Streaming ao vivo situações de exploração e abuso sexual de crianças</p>	<p>Trata-se da transmissão em tempo real de situações de exploração e abuso sexual de crianças pela Internet.</p>
<p>Imagens Geradas por Computador (CGI – Computer-Generated Imagery)</p>	<p>No contexto de abuso e exploração sexual de crianças, refere-se a imagens sexualizadas de crianças, total ou parcialmente criadas de forma artificial ou digital.³⁹⁰</p>
<p>"Deepfake"</p>	<p>Trata-se de uma forma de CGI que utiliza a inteligência artificial para substituir a imagem de uma pessoa por outra em fotos ou vídeos gravados.³⁹¹</p>
<p>"Capping"</p>	<p>Trata-se de abusadores que capta imagens de transmissões ao vivo de situações de abuso e exploração sexual de crianças.³⁹²</p> <p>O "capping" inclui igualmente os abusadores que captam imagens inócuas de crianças e as usam para fins sexuais (convertendo-as em imagens sexualizadas de crianças).</p>
<p>"Gamificação" do abuso</p>	<p>É a aplicação de elementos semelhantes ao jogo (por exemplo, pontuação, competição com outros, regras de jogo) para encorajar a participação em situações de abuso e exploração.</p>

Termo	Definição
Criança que exibindo comportamento sexual danoso	Trata-se de uma criança ou jovem com menos de 18 anos de idade que apresenta comportamentos inadequados do ponto de vista do seu estágio de desenvolvimento, que podem ser danosos para si ou para os outros e/ou resultar em abuso sobre outra criança, jovem ou adulto. ³⁹³
Fatores de risco	Fatores ao nível individual, de relacionamento, da comunidade e da sociedade que podem aumentar a probabilidade de uma criança sofrer abuso e exploração sexual.
Fatores de proteção	Fatores ao nível individual, de relacionamento, da comunidade e da sociedade que podem reduzir o risco de uma criança se tornar vítima de abuso e exploração sexual.
Revitimização	Quando uma vítima enfrenta qualquer tipo de abuso sexual ou agressão subsequente ao primeiro abuso ou agressão. ³⁹⁴ Esta situação inclui a posterior distribuição e visualização de imagens na Internet: uma única imagem de uma vítima pode ser partilhada centenas ou milhares de vezes. ³⁹⁵ A revitimização pode ser causada pelo mesmo abusador ou por outro que não o responsável pela vitimização inicial.
Tráfico de crianças	Refere-se ao recrutamento, transporte, transferência, abrigo ou acolhimento de uma criança para fins de exploração. ³⁹⁶
Hemisfério Norte	Os países do G8, os Estados Unidos, o Canadá, todos os Estados-Membros 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, exceto a China. ³⁹⁷
Hemisfério Sul	África, América Latina, Médio Oriente e Ásia em vias de desenvolvimento — inclui três das quatro novas economias avançadas dos países do BRIC (excluindo a Rússia): o Brasil, a Índia e a China. ³⁹⁸
Web de superfície (Surface web)	A parte da web prontamente disponível para o público em geral e pesquisável com os normais motores de pesquisa da web. ³⁹⁹
Deep web	A parte da web cujo conteúdo não é indexado pelos motores de pesquisa vulgares de Internet e que inclui muitas utilizações comuns, como o webmail, o homebanking e os serviços de subscrição. O conteúdo é localizado e acedido através de link direto ou endereço IP e pode exigir uma palavra-passe ou outro acesso de segurança para lá da página pública da web. ⁴⁰⁰
Dark web	A camada de informações e páginas que só podem ser acedidas por meio das chamadas "redes de sobreposição" (como as Redes Privadas Virtuais (VPN) e redes de partilha de ficheiros ponto a ponto (P2P)) que obscurecem o acesso público. Os utilizadores precisam de um software especial para aceder à dark web porque grande parte desta é encriptada sendo que o alojamento da maioria das páginas na dark web é anónimo. ⁴⁰¹

Termo	Definição
Tecnologias de Segurança (Safety Tech)	Soluções tecnológicas que facilitam uma experiência online mais segura, e protegem os utilizadores de conteúdos, contactos ou condutas danosas. ⁴⁰³
Safety-by-design	A incorporação dos direitos e da segurança dos utilizadores na conceção e no modo de funcionamento dos produtos e dos serviços online, desde a sua criação. ⁴⁰³
Peer-to-peer (P2P)	Numa rede P2P, os “peers” (pares) são sistemas informáticos conectados entre si via Internet. Os ficheiros podem se partilhados diretamente entre os sistemas na rede sem a necessidade de um servidor central. Por outras palavras, cada computador numa rede P2P torna-se um servidor de ficheiros e também um cliente. ⁴⁰⁴
Virtual Private Network (VPN)	Uma Rede Privada Virtual é uma tramitação que cria uma conexão encriptada pela Internet desde um dispositivo até uma rede, conhecido como túnel. ⁴⁰⁵
Hashing	Um processo pelo qual um hash binário é criado por um algoritmo matemático que transforma os dados de qualquer dimensão em dados de comprimento fixo bastante mais curtos. Esta sequência mais curta representa os dados originais e torna-se a assinatura exclusiva desse ficheiro, ou seu valor hash — frequentemente chamado de impressão digital. ⁴⁰⁶
Hash-matching	Um processo de utilização de bases de dados de material de abuso sexual infantil codificadas por hash para detetar quando o material é partilhado novamente, comparando seu valor de hash com aqueles de ficheiros já conhecidos. ⁴⁰⁷
Classificação por Inteligência Artificial (AI) ou moderação por AI	Sistemas de moderação total ou parcialmente automatizados que identificam o conteúdo abusivo de acordo com regras determinadas e interpretando diferentes exemplos de conteúdo que é ou não é abusivo. ⁴⁰⁸
Encriptação	Trata-se do processo de codificação de informação para uma forma alternativa que só pode ser decodificada por pessoas autorizadas que possuam a chave de desencriptação. ⁴⁰⁹
Encriptação end-to-end	Trata-se de uma forma de encriptação em que o conteúdo de cada mensagem é visível apenas para o remetente e para o destinatário. A decodificação da mensagem requer uma chave de desencriptação privada trocada apenas entre os correspondentes, de modo a que, ainda que a mensagem possa ser interceptada, a mesma não pode ser visualizada nem monitorizada pelo prestador do serviço, pelas autoridades policiais ou por terceiros. ⁴¹⁰
"Serviços ocultos"	Sites que são alojados numa rede proxy (como a Tor), pelo que a sua localização não é rastreável. ⁴¹¹
Metadados	Dados que descrevem outros dados. ⁴¹² Exemplos de metadados: tempo e duração de uma chamada telefónica (em oposição ao conteúdo da própria comunicação).
Tor	Rede de privacidade de código aberto que permite aos utilizadores navegarem anonimamente na Internet. O sistema utiliza uma série de nós em camadas para ocultar o URL, dados online e o histórico de navegação. ²²⁷

Termo	Definição
Secure tooling (Uso de ferramentas seguras)	Software/aplicações utilizadas para contribuir para o anonimato online, ocultando a localização do utilizador e a sua identidade.
Sistemas Operativos Seguros	A utilização de sistemas operativos que podem ser iniciados a partir de um disco USB. Uma vez que não efetuam gravação no disco rígido, assim que forem desligados, tudo é eliminado. O software de encriptação pode então ser utilizado para proteger o conteúdo de um ficheiro e partes do disco que só podem ser acedidos com a chave de desencriptação do utilizador.
Tradecraft	Trata-se de um conjunto de técnicas de camuflagem e estratégias de evasão, em permanente evolução, que os abusadores utilizam para evitar a deteção pessoal e as respetivas técnicas e estratégias para identificar e envolver as crianças.
Emulação e Virtualização	As máquinas virtuais permitem que os utilizadores corram um sistema operativo que se comporta como um computador totalmente separado numa janela de aplicação no seu desktop. Alguns emuladores criam um interface virtual de smartphone no computador. Isto permite que o utilizador instale e use programas e aplicações no seu computador que, de outra forma, não estariam disponíveis. Os emuladores são frequentemente usados em conjunto com ferramentas de "capping" pois evitam que a notificação de "captura do ecrã" seja enviada para a vítima, enquanto que o abusador pode usar o software de "capping" instalado no próprio computador para captar imagens mais nítidas.
Convenção das Nações Unidas sobre os Direitos da Criança	Tratado internacional de direitos humanos composto por 54 artigos que cobrem todos os aspetos da vida de uma criança, estabelecendo os direitos civis, políticos, económicos, sociais e culturais aos quais todas as crianças têm direito. Explica ainda como os adultos e os governos devem trabalhar em conjunto para garantir que todas as crianças possam usufruir de todos os direitos que lhes assistem. ^{414 415}
Comentário 25 do Comité das Nações Unidas sobre os Direitos da Criança	Diretriz vinculativa que define a forma como os Direitos da Criança se aplicam no ambiente digital. Ajuda os Estados a compreenderem as etapas que são necessárias para fazer respeitar, proteger e cumprir os direitos das crianças no ambiente digital. ⁴¹⁶
Princípios Voluntários para o Combate ao Abuso e Exploração Sexual de Crianças	Trata-se de um conjunto de princípios que definem um enquadramento para a exploração e o abuso sexual de crianças online, e visam impulsionar a ação coletiva. Foram desenvolvidos por cinco Governos (Austrália, Canadá, Nova Zelândia, Reino Unido e EUA), com a consulta de um conjunto alargado de partes interessadas, incluindo um grupo líder de representantes do setor. ⁴¹⁷
WeProtect Global Alliance Model National Response (MNR)	Trata-se de um modelo de enquadramento que orienta e apoia os países e organizações na prossecução de uma resposta nacional (MNR). O modelo está centrado na ajuda aos países para que estes possam estruturar a sua resposta ao problema da exploração sexual de crianças online. ⁴¹⁸
WeProtect Global Alliance Global Strategic Response (GSR)	Trata-se de um modelo de enquadramento que orienta e apoio os países e organizações na prossecução de uma resposta estratégica global (GSR). O modelo está centrado na melhoria da cooperação global para dar resposta ao problema da exploração sexual de crianças online.
Convenção do Conselho da Europa para a Proteção de Crianças contra a Exploração Sexual e o Abuso Sexual (também conhecida como "Convenção de Lanzarote")	Uma convenção que exige a criminalização de todos os tipos de crimes sexuais contra crianças. Estabelece também que os Estados, na Europa e fora dela, devem adotar legislação específica e tomar medidas adequadas para prevenir a violência sexual, para proteger as crianças vítimas da mesma e para condenar os respetivos autores. O "Comité de Lanzarote" é o órgão criado para monitorizar a implementação efetiva da Convenção de Lanzarote pela partes para a identificação de boas práticas neste âmbito. ⁴¹⁹
Directiva europeia relativa à privacidade e às comunicações electrónicas (European e-Privacy Directive)	Legislação que diz respeito ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas. ⁴²⁰ A Diretiva não contém uma base legal explícita para prosseguir as atuais as práticas voluntárias para detetar, denunciar e eliminar o abuso sexual de crianças. ⁴²¹

10

Anexo A:

Conclusões do Inquérito pela WeProtect Global Alliance/Technology Coalition às empresas tecnológicas

RESUMO DAS CONCLUSÕES

Muitas das empresas inquiridas dispõem de recursos para detetar o abuso e a exploração sexual de crianças online bem como de mecanismos de denúncia, sendo que existem oportunidades para reforçar a colaboração e concentrar maior esforço na dissuasão e na prevenção deste tipo de crimes.

	Reporting	Detection	Deterrence and prevention	Tool development	Transparency reporting
Key findings	Most reports are at least partly automated, and almost all companies have some form of reporting mechanism	The majority of companies are using hash-based tools to detect both image and video child sexual abuse materia. Use of advanced classifiers to detect video and livestream content, is less common despite the fact this category is becoming more prevalent	Prevention measures such as deterrence messaging and child safety resources are widely provided, but these are less common than use of hash-based detection, despite their potential to prevent abuse before it occurs	Many companies use tools developed by others, but it is less common for them to develop tools in-house and share them	Most companies do not yet publish transparency reports. However, of companies that do, a large majority publish specific data on child sexual abuse and exploitation
Recommendations	Diversify reporting pathways to gain a more holistic picture of the threat	Share information and intelligence (e.g. hashes and keywords) to help stay ahead of what is a rapidly evolving space	Invest in deterrence and prevention measures, and diversify the targeting of online safety resources to avoid over-reliance on one group, to help prevent abuse before it occurs	Collaborate and share tools across industry to help maximise their benefit. Ensure regulatory frameworks empower rather than hinder companies utilising key tools	Develop universal reporting frames to ensure data is consistent and encourage more companies to make it publicly available

METODOLOGIA

Entre fevereiro e março de 2021, a WeProtect Global Alliance e a Technology Coalition conduziram um inquérito com 20 perguntas junto dos respetivos membros do setor para compreender a abrangência das atividades desenvolvidas pelas empresas de tecnologia no combate ao abuso sexual de crianças online. No total, 32 empresas responderam, tratando-se de empresas com dimensões variadas desde menos de 250 funcionários até mais de 5000.



LIMITAÇÕES

A amostra é pequena tendo em conta a dimensão do setor global de tecnologias, sendo mais representativa das empresas baseadas no Hemisfério Norte. Contudo, a ampla diversidade de dimensões e tipos de empresas fornece, indiscutivelmente, uma amostra representativa deste setor. Uma vez que o inquérito foi completamente anónimo e agregado, não foi possível associar as respostas de um inquirido a várias perguntas, limitando o potencial de comparação entre respostas — por exemplo, para as empresas de diferentes dimensões. Constatou-se também que algumas das perguntas podem não ter sido relevantes para todos os inquiridos, sendo que tal foi atenuado pela inclusão da opção de resposta "não relevante" ou permitindo que as perguntas sejam ignoradas.

RESULTADOS INTEGRAIS

Elaboração de relatórios:

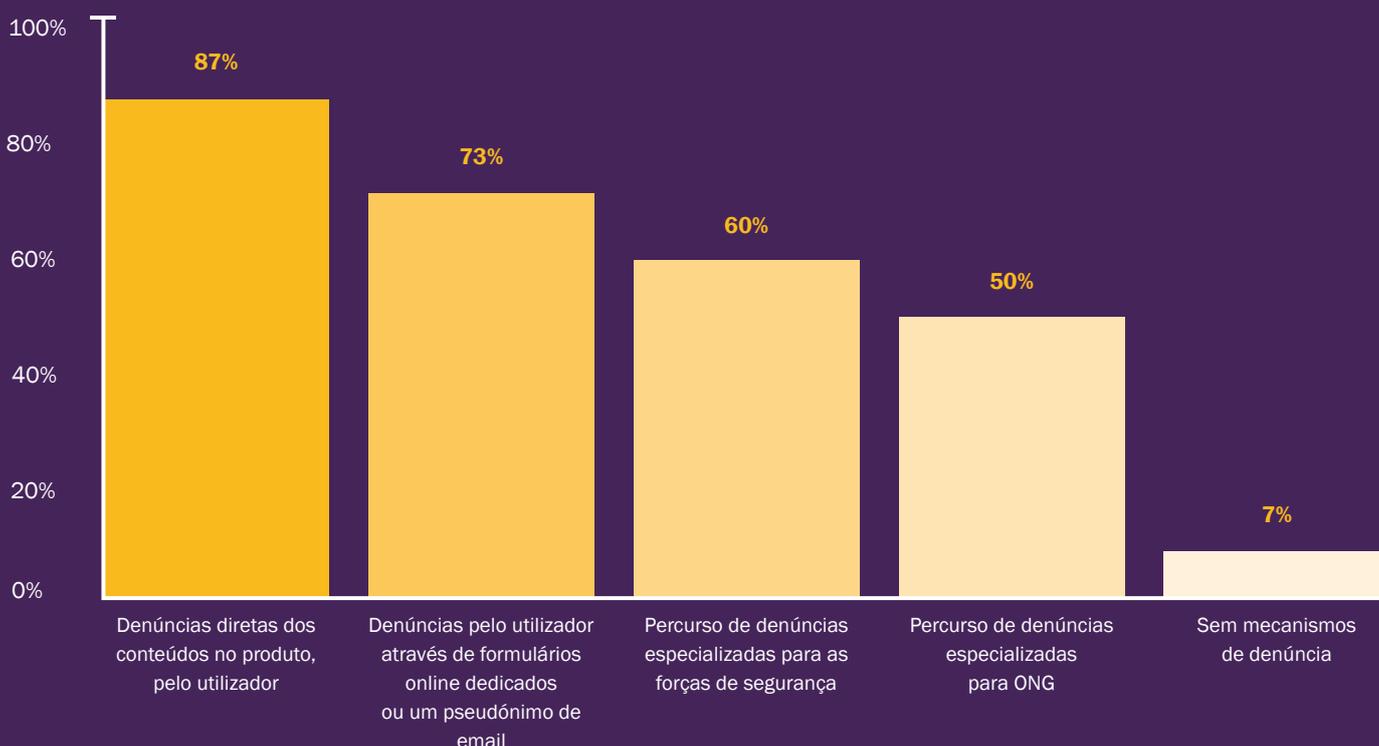
84% das empresas inquiridas dispõe, pelo menos parcialmente, de processos automatizados para encaminhar as denúncias de abuso sexual de crianças online, o que sugere que a gestão de denúncias seja relativamente eficiente.

Esta pergunta não se concentrou nos mecanismos de detecção proativa que as empresas possam ter em vigor, como tal, não apresenta uma panorâmica global a este respeito. Contudo, excluindo este aspeto, o mecanismo de denúncia mais popular para as empresas são as denúncias diretas apresentadas pelos utilizadores. Os mecanismos menos populares são os caminhos de denúncias para as ONGs e as forças da lei, sugerindo que há espaço para uma maior colaboração intersetorial. Diversificar as vias de denúncia evitará a dependência excessiva das denúncias dos utilizadores, o que, dadas as baixas taxas de autodenúncia, pode ajudar a fornecer um quadro mais completo do delito.



Figura 19: Mecanismos que as empresas disponibilizam para permitir a denúncia.

Que mecanismos disponibilizam as empresas para facilitar a denúncia de material de abuso sexual de crianças?

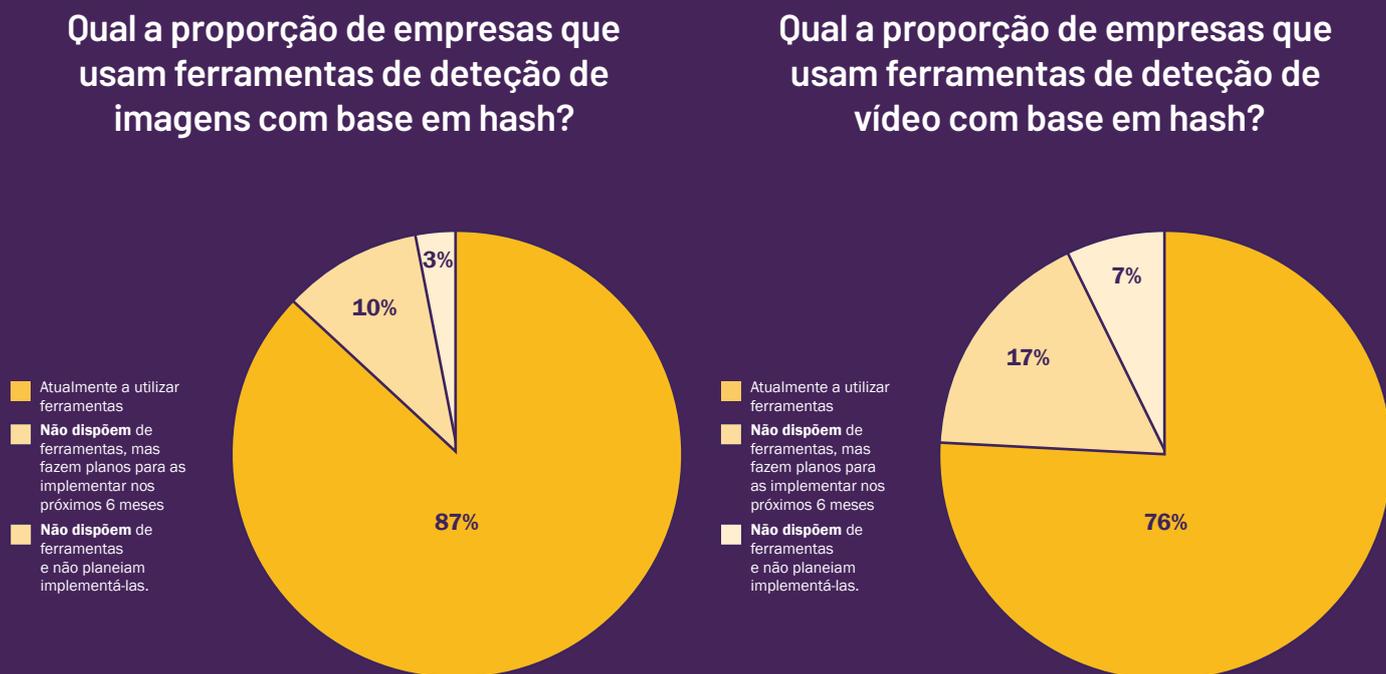


DETEÇÃO

Deteção com base em hash

A maioria dos inquiridos utiliza ferramentas baseadas em hash para detetar imagens e vídeos de abuso sexual de crianças nas respetivas plataformas. A maior parte daqueles que ainda não usam ferramentas baseadas em hash planeia implementá-las nos próximos seis meses, conforme indicado na Figura 20, abaixo.

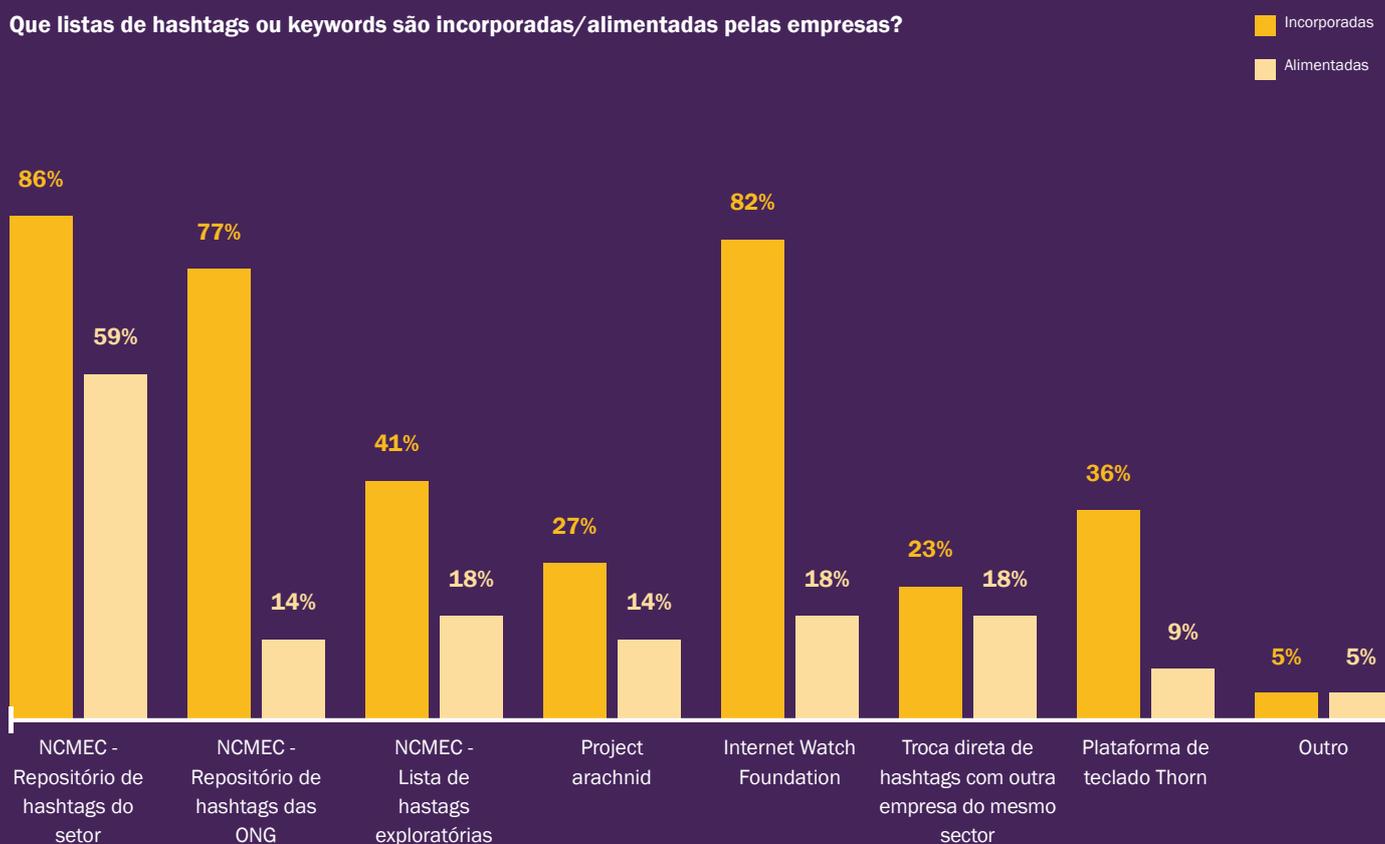
Figura 20: Utilização de ferramentas de deteção com base em hash pelas empresas



Para uma utilização eficaz das ferramentas de deteção baseadas em hash, as empresas precisam de ter acesso a hashes de materiais conhecidos de abuso sexual de crianças. Um outro elemento importante para a deteção é a capacidade de bloquear os termos de pesquisa relacionados com o abuso sexual de crianças, e para os quais as empresas precisam de aceder às listas de keywords.

A maioria das empresas recolhe hashes e keywords de, pelo menos, um repositório, conforme mostrado na Figura 21, abaixo. No entanto, é muito menor a percentagem de empresas que contribui com hashes ou keywords. Partindo do princípio que as empresas não estão a detetar apenas conteúdos já conhecidos, a partilha limitada de informações de inteligência externas acaba por afetar a capacidade para acompanhar o ritmo de evolução da ameaça.

Figura 21: Utilização de listas de hash/keywords pelas empresas

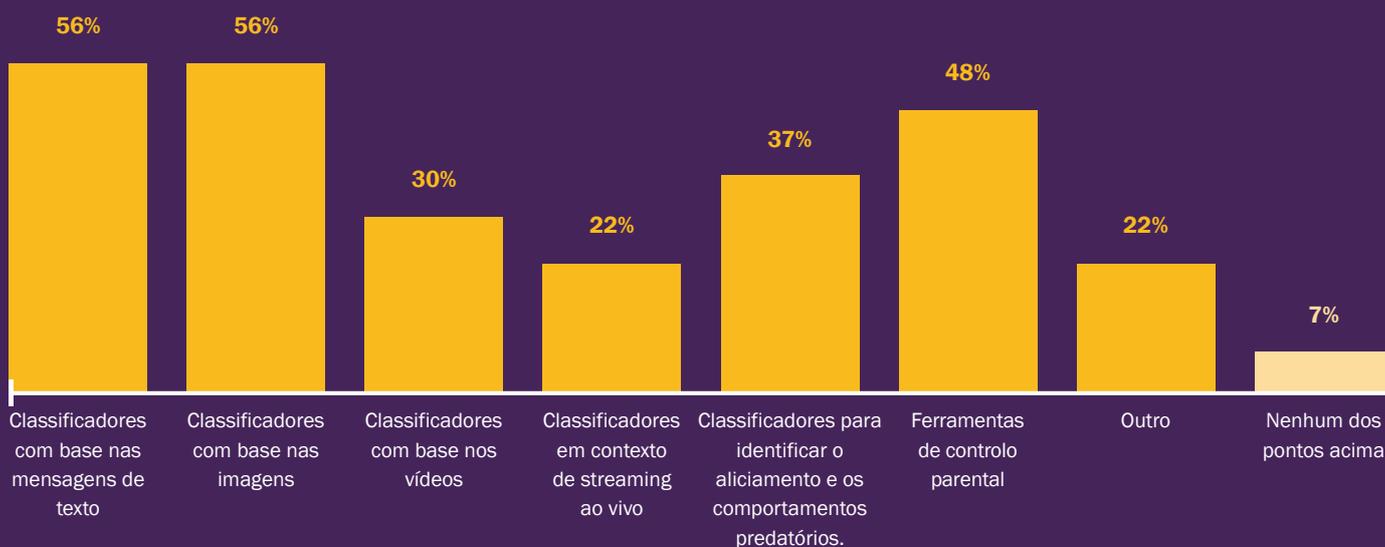


DETEÇÃO AVANÇADA:

A detecção avançada refere-se a tecnologias como sejam os classificadores de inteligência artificial. Estas medidas de detecção avançadas são usadas menos frequentemente do que as medidas de detecção baseadas em "hashing". Apesar das evidências que indicam o aumento da prevalência dos conteúdos de vídeo e de transmissão ao vivo, os classificadores que detetam esse tipo de materiais são utilizados por apenas 30% e 22% dos inquiridos, respetivamente.

Figura 22: Medidas adicionais de combate à exploração e abuso sexual online.

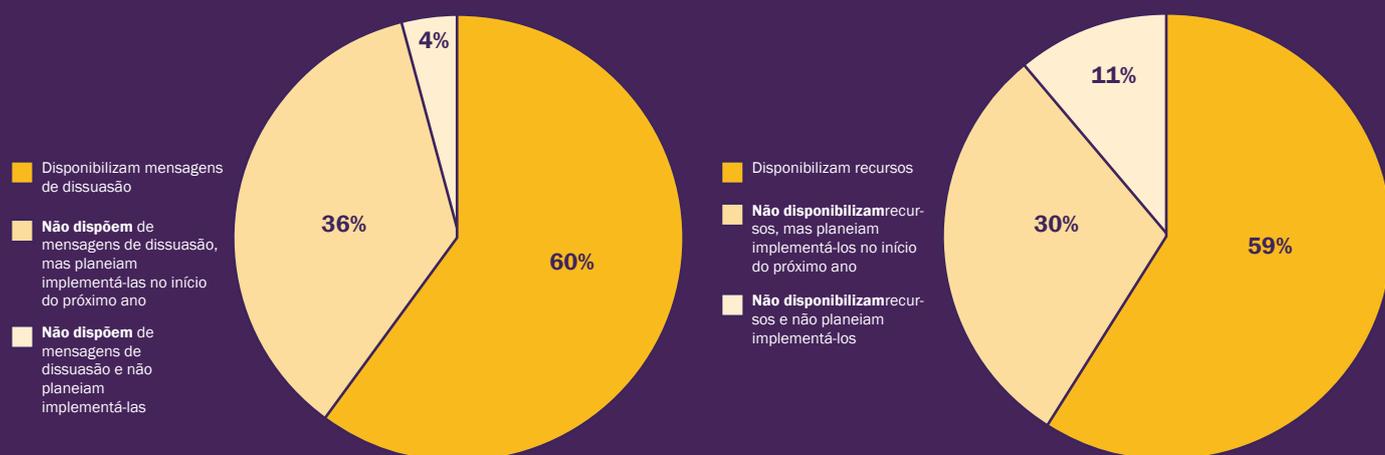
Que medidas adicionais utilizam as empresas para combater a exploração e abuso sexual online?



DISSUAÇÃO E PREVENÇÃO

A maioria dos inquiridos emite mensagens de dissuasão dirigidas a potenciais abusadores e disponibiliza recursos online para a segurança infantil numa ação preventiva do abuso, contudo ambos são menos comuns do que os mecanismos para deteção de material de abuso sexual de crianças.

Figura 23: Utilização pelas empresas de mensagens de dissuasão e de recursos de segurança online das crianças.



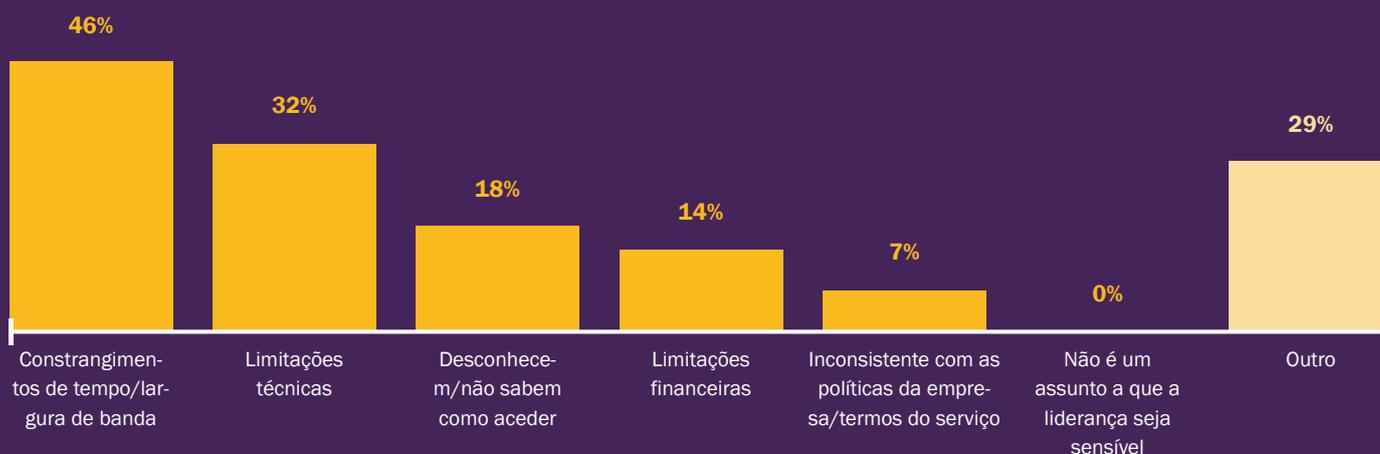
O inquérito constatou que a maioria dos recursos online de segurança infantil são dirigidos aos pais, o que é positivo, uma vez que estes são, geralmente, o primeiro ponto de contacto para uma criança que esteja a experienciar sofrimento online.⁴²² Contudo, as evidências sugerem também que a exploração e o abuso sexual infantil são frequentemente ser praticados por familiares.⁴²³ Para apoiar essas vítimas e evitar a dependência excessiva de um grupo para salvaguardar as crianças, é possível disponibilizar mais recursos dirigidos às próprias crianças, aos educadores e a outros públicos.

DESENVOLVIMENTO DE FERRAMENTAS:

Quase 50% das empresas inquiridas utilizam classificadores de conteúdo desenvolvidos por outras empresas, mas apenas 26% disponibilizam o acesso a terceiros das ferramentas por si desenvolvidas. Seria necessária uma investigação mais aprofundada para compreender as razões para este fenómeno. Uma maior colaboração e partilha de ferramentas, sempre que possível, ajudaria certamente a maximizar o benefício geral das ferramentas.

Figura 24: Barreiras ao uso de ferramentas de combate ao abuso sexual de crianças online.

Que obstáculos enfrentam as empresas na utilização de recursos técnicos para combater a exploração e abuso sexual online?



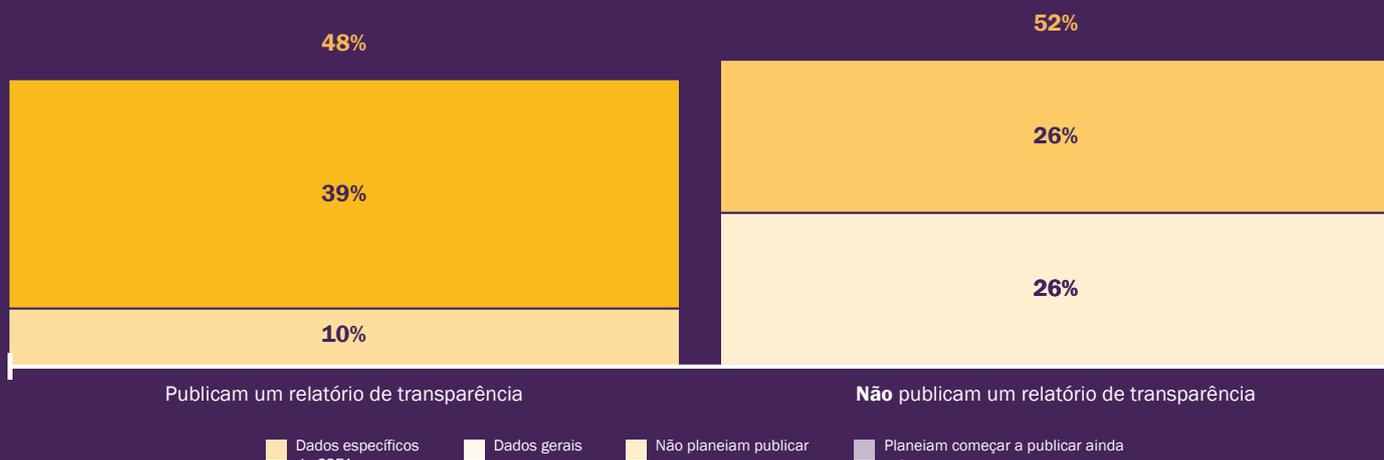
As restrições de tempo e largura de banda são as principais barreiras para as empresas que desenvolvem e implementam ferramentas de combate ao abuso sexual de crianças online. A falta de adesão por parte das chefias não foi citada como uma dificuldade por nenhum dos inquiridos.

TRANSPARÊNCIA

É crucial criar uma cultura de transparência que permita uma resposta conjunta e informada à exploração sexual e ao abuso de crianças online. No entanto, apenas 49% dos inquiridos publicam regularmente um relatório de transparência. Destes, 80% publicam dados específicos sobre exploração e abuso sexual infantil, o que é fundamental para entender a escala e a amplitude da ameaça.

Figura 25: Relatórios Empresariais sobre Transparência

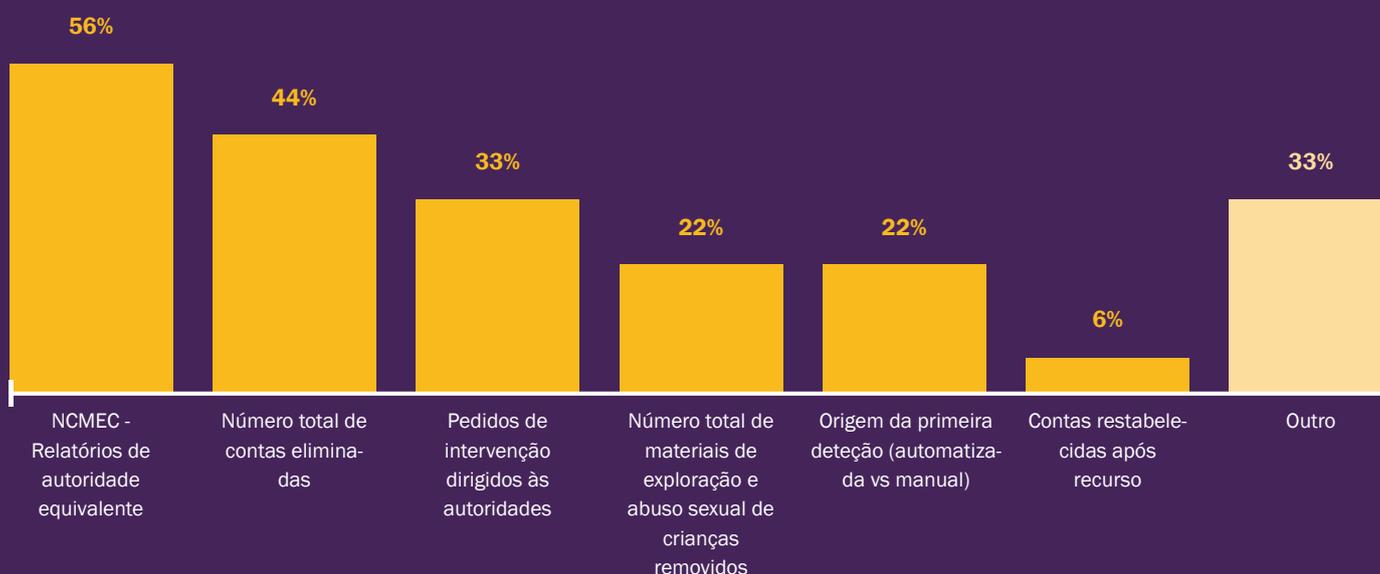
Qual a percentagem de empresas que publicam regularmente relatórios de transparência relativamente à incidência de conteúdos de exploração e abuso sexual de crianças, nas respetivas plataformas?



Os dados reportados pelas empresas variam, conforme mostrado na Figura 26, abaixo. Será necessário um maior empenho no desenvolvimento de estruturas universais de reporte. Tal permitiria que os dados fossem consistentes e comparáveis, incentivando as empresas que ainda não publicam dados, a disponibilizá-los publicamente.

Figura 26: Tipos de dados incluídos nos relatórios de transparência.

De entre as empresas que publicam um relatório de transparência, quais os tipos de dados incluídos relativamente à exploração e abuso sexual de crianças?



A Figura 26 mostra que é frequente as empresas reportarem dados agregados, como sejam o total de peças de material de abuso sexual de crianças que foi removido. No entanto, os resultados dos relatórios de transparência raramente são desagregados de modo a mostrar a prevalência de diferentes tipos de abuso sexual de crianças, como o aliciamento ou a prática de transmissões ao vivo. A exposição desses números permitiria obter uma visão mais informada sobre o contexto em que os diferentes tipos de danos proliferam, permitindo assim realizar intervenções mais direcionadas de acordo com as reais necessidades no terreno.

References

- 1 Annual Report 2020 (INHOPE, 2021) Accessed from: <https://inhope.org/media/pages/the-facts/download-our-whitepapers/c16bc4d839-1620144551/inhope-annual-report-2020.pdf> 06/05/2021
- 2 4 arrested in takedown of dark web child abuse platform with some half a million users (Europol, 2021) Accessed from: <https://www.europol.europa.eu/newsroom/news/4-arrested-in-takedown-of-dark-web-child-abuse-platform-some-half-million-users> 04/05/2021
- 3 NetClean Report COVID-19 Impact 2020 (NetClean, 2020) Accessed from: <https://www.netclean.com/netclean-report-2020/#> 04/05/2021
- 4 Fighting Child Exploitation with Big Data (Freethink, 2020) Accessed from: <https://www.freethink.com/videos/child-exploitation> 16/06/2021
- 5 Falling short: demand side sentencing for online sexual exploitation of children (International Justice Mission, 2020) Accessed from: <https://www.ijmuk.org/images/EMBARGO-8-NOV-20-IJM-REPORT-FALLING-SHORT-Demand-Side-Sentencing-for-Online-Sexual-Exploitation-of-Children.pdf> 15/02/2021
- 6 Online child sexual abuse activity has increased (NetClean, 2021) Accessed from: <https://www.netclean.com/netclean-report-2020/insight-2/> 26/01/2021
- 7 Online enticement reports skyrocket in 2020 (NCMEC, 2021) Accessed from: <https://www.missingkids.org/blog/2021/online-enticement-reports-skyrocket-in-2020> 24/02/2021
- 8 IWF Annual Report: 2020 Trends and Data (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends> 22/04/2021
- 9 Research report: The impact of COVID-19 on the risk of online child sexual exploitation and the implications for child protection and policing (University of New South Wales, Sydney, 2021) Accessed from: https://www.arts.unsw.edu.au/sites/default/files/documents/eSafety-OCSE-pandemic-report-salter-and-wong.pdf?utm_source=ActiveCampaign&utm_medium=email&utm_content=New+briefings+and+reports+from+the+Alliance+and+our+members&utm_campaign=May+2021+newsletter 07/06/2021
- 10 COVID-19: Child sexual exploitation and abuse threats and trends (Interpol, 2020) Accessed from: <https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-highlights-impact-of-COVID-19-on-child-sexual-abuse> 26/01/2021
- 11 By the Numbers (NCMEC, 2021) Accessed from: <https://www.missingkids.org/gethelpnow/cybertipline> 16/06/2021
- 12 IWF Annual Report: Self-generated child sexual abuse (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/selfgenerated> 06/05/2021
- 13 Acion to end Child Sexual Abuse and Exploitation (UNICEF, 2020) Accessed from: <https://www.unicef.org/media/89206/file/CSAE-Brief-v3.pdf> 23/07/2021
- 14 Survey of Technology Companies (WeProtect Global Alliance and Technology Coalition, 2021) See Annex A: Findings from WeProtect Global Alliance/Technology Coalition Survey of Technology Companies
- 15 IWF Annual Report: Hidden Services (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/Trends/International/Other/Hidden> 22/04
- 16 PA Consulting engagement with Australian Centre to Counter Child Exploitation, 01/03/2021
- 17 Violencia sexual a menores ya deja mas de mil victimas en lo corrido de 2021 (LAFM, 2021) Accessed from: <https://www.lafm.com.co/colombia/violencia-sexual-menores-ya-deja-mas-de-mil-victimmas-en-lo-corrido-de-2021> 11/03/2021
- 18 Abuso sexual en internet y redes de trata (Infobae, 2020) Accessed from: <https://www.infobae.com/america/mexico/2020/07/27/abuso-sexual-en-internet-y-redes-de-trata-los-crimenes-contra-la-ninez-que-aumentaron-durante-la-pandemia/> 25/02/2021
- 19 Production and distribution of child sexual abuse material by parental figures (Australian Institute of Criminology, 2021) Accessed from: https://www.aic.gov.au/sites/default/files/2021-02/ti616_production_and_distribution_of_child_sexual_abuse_material_by_parental_figures.pdf 09/03/2021
- 20 Los casos de abuso sexual contra menores en espana se multiplican por 4 en la ultima decada (Levante, 2021) Accessed from: <https://protect-eu.mimecast.com/s/WuEPCWn-WgFxBY3Hxchqm?domain=levante-emv.com> 23/02/2021
- 21 Falling short: demand side sentencing for online sexual exploitation of children (International Justice Mission, 2020) Accessed from: <https://www.ijmuk.org/images/EMBARGO-8-NOV-20-IJM-REPORT-FALLING-SHORT-Demand-Side-Sentencing-for-Online-Sexual-Exploitation-of-Children.pdf> 15/02/2021

- 22 A Global Strategic Response to Online Child Sexual Exploitation and Abuse (WeProtect Global Alliance, 2021) Accessed from: <https://www.weprotect.org/wp-content/uploads/WeProtectGA-Global-Strategic-Response-EN.pdf> 17/06/2021
- 23 Action to end Child Sexual Abuse and Exploitation (UNICEF/ End Violence Against Children, 2020) Accessed from <https://www.unicef.org/media/89206/file/CSAE-Brief-v3.pdf> 13/05/2021
- 24 Guidelines for Medico-Legal Care for Victims of Sexual Violence: Child Sexual Abuse (World Health Organisation, 2003) Accessed from: https://www.who.int/violence_injury_prevention/publications/violence/med_leg_guidelines/en/ 19/04/2021
- 25 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (ECPAT, 2016) Accessed from: https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines_en.pdf 25/05/2021
- 26 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Interagency Working Group on Sexual Exploitation of Children, 2016) Accessed from: https://www.ecpat.org/wp-content/uploads/2016/12/Terminology-guidelines_ENG.pdf (23/07/2021)
- 27 Global Threat Assessment 2019 (WeProtect Global Alliance, 2019) Accessed from: <https://www.weprotect.org/issue/global-threat-assessment/> 26/01/2021
- 28 Grooming (NSPCC) Accessed from: <https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/grooming/> 25/05/2021
- 29 Online Enticement (NCMEC) Accessed from: <https://www.missingkids.org/netsmartz/topics/onlineenticement> 25/05/2021
- 30 Netclean Annual Report; Comment to insight 4 – Simon Bailey (Netclean, 2020) Accessed from: <https://www.netclean.com/netclean-report-2020/insight-6/> 17/06/2021
- 31 Netclean Annual Report; Insight 2: Online Child Sexual Abuse Activity has increased (Netclean, 2020) Accessed from: <https://www.netclean.com/netclean-report-2020/insight-2/> 07/06/2021
- 32 Netclean Annual Report; Comment to insight 4 – Rob Jones (Netclean, 2020) Accessed from: <https://www.netclean.com/netclean-report-2020/insight-6/> 17/06/2021
- 33 Impact of coronavirus disease on different manifestations of sale and sexual exploitation of children (United Nations, 2021) Accessed from: https://reliefweb.int/sites/reliefweb.int/files/resources/A_HRC_46_31_E.pdf 07/06/2021
- 34 Protection of children should always trump protection of privacy (eSafety Commissioner, 2020) Accessed from: <https://www.esafety.gov.au/about-us/blog/protecting-children-should-always-trump-protecting-privacy> 07/06/2021
- 35 Abuso sexual infantil crece en un 50% durante la pandemia por coronavirus (El Imparcial, 2021) Accessed from: <https://www.elimparcial.com/mundo/Abuso-sexual-infantil-crece-en-un-50-durante-la-pandemia-por-coronavirus-20210216-0011.html> 07/06/2021
- 36 Online sexual abuse of children rising amid COVID 19 pandemic – Save the Children Philippines (Relief Web, 2021) Accessed from: <https://reliefweb.int/report/philippines/online-sexual-abuse-children-rising-amid-covid-19-pandemic-save-children> 22/04/2021
- 37 La pornografía infantil creció 117% en México (Jornada, 2020) Accessed from: <https://www.jornada.com.mx/2020/08/10/politica/010n1pol> 07/06/2021
- 38 Ending Violence Against Children and COVID-19 (Child Rights Now!, 2020) Accessed from: https://www.wvi.org/sites/default/files/2020-07/2020_06_JF_CRN_Ending%20Violence%20Against%20Children%20and%20COVID%2019%20ENG.pdf 07/06/2021
- 39 COVID-19 Conversations: The Crisis of Online Child Sexual Exploitation (Equality Now, 2020) Accessed from: https://www.equalitynow.org/covid_19_online_exploitation 07/06/2021
- 40 Keeping Children Safe in Uganda’s COVID-19 Response (Save the Children, 2020) Accessed from: <https://resourcecentre.savethechildren.net/node/17615/pdf/Joining%20Forces%20-%20Protecting%20children%20during%20Covid-19%20in%20Uganda.pdf> 08/06/2021
- 41 La violencia contra los niños aumenta con la covid (Inter Press Service, 2021) Accessed from: <https://ipsnoticias.net/2021/04/la-violencia-los-ninos-aumenta-la-covid/> 11/06/2021
- 42 Child Sexual Exploitation Materials Hotline Annual Report 2020 (EOKM, 2021) Accessed from: <https://www.eokm.nl/wp-content/uploads/2021/04/EOKM-Jaarverslag-2020-DEF-ENG.pdf> 17/06/2021
- 43 National Strategic Assessment of Serious and Organised Crime (National Crime Agency, 2021) Received by email from the NCA, 25/05/2021
- 44 Pedophilia and Sexual Offending Against Children: Theory, Assessment, and Intervention, Second Edition (Michael Seto, 2018)
- 45 Research report: The impact of COVID-19 on the risk of online child sexual exploitation and the implications for child protection and policing (University of New South Wales, Sydney, 2021) Accessed from: https://www.arts.unsw.edu.au/sites/default/files/documents/eSafety-OCSE-pandemic-report-salter-and-wong.pdf?utm_source=ActiveCampaign&utm_medium=email&utm_content=New+briefings+and+reports+from+the+Alliance+and+our+members&utm_campaign=May+2021+newsletter 07/06/2021
- 46 IWF Annual Report 2020: Hidden Services (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/other/hidden> 07/06/2021

- 47 Europol Serious and Organised Crime Threat Assessment (SOCTA) 2021 (Europol, 2021) Accessed from: <https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-20/04/2021>
- 48 Why Children are at risk of sexual exploitation during COVID-19 (ECPAT International, 2020) Accessed from: <https://ecpat.exposure.co/covid19?embed=true> 07/06/2021
- 49 Europol Serious and Organised Crime Threat Assessment (SOCTA) 2021 (Europol, 2021) Accessed from: <https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-20/04/2021>
- 50 Netclean Annual Report 2020; Insight 4: Moderate increase in actual investigations and cases (Netclean, 2020) Accessed from: <https://www.netclean.com/netclean-report-2020/insight-4/> 06/05/2021
- 51 COVID-19 to add as many as 150 million extreme poor by 2021 (World Bank, 2020) Accessed from: <https://www.worldbank.org/en/news/press-release/2020/10/07/covid-19-to-add-as-many-as-150-million-extreme-poor-by-2021> 06/07/2021
- 52 Joint Leaders' statement – Violence against children: A hidden crisis of the COVID-19 pandemic (World Health Organisation, 2020) Accessed from: <https://www.who.int/news/item/08-04-2020-joint-leader-s-statement--violence-against-children-a-hidden-crisis-of-the-covid-19-pandemic> 07/06/2021
- 53 Children's screen time has soared in the pandemic, alarming parents and researchers (NY Times, 2021) Accessed from: <https://www.nytimes.com/2021/01/16/health/covid-kids-tech-use.html> 16/07/2021
- 54 Children at increased online risk during COVID-19 pandemic (UNICEF, 2020) Accessed from: <https://www.unicef.org/bhutan/press-releases/children-increased-online-risk-during-covid-19-pandemic> 16/07/2021
- 55 The impact of the coronavirus pandemic on child welfare: sexual abuse (NSPCC, 2020) Accessed from: <https://learning.nspcc.org.uk/media/2280/impact-of-coronavirus-pandemic-on-child-welfare-sexual-abuse.pdf> 16/07/2021
- 56 Aumentan casos de abuso infantil tras relajarse medidas en Paraguay (Prensa Latina, 2021) Accessed from: <https://www.prensa-latina.cu/index.php?o=rn&id=437283> 07/06/2021
- 57 Impact of coronavirus disease on different manifestations of sale and sexual exploitation of children (United Nations, 2021) Accessed from: https://reliefweb.int/sites/reliefweb.int/files/resources/A_HRC_46_31_E.pdf 07/06/2021
- 58 Child protection in the time of COVID-19 (Australian Institute of Health and Welfare, 2021) Accessed from: <https://www.aihw.gov.au/reports/child-protection/child-protection-in-the-time-of-covid-19/summary> 16/06/2021
- 59 Protecting children from violence in the time of COVID-19: Disruptions in prevention and response services (Unicef, 2020) Accessed from: <https://www.unicef.org/reports/protecting-children-from-violence-covid-19-disruptions-in-prevention-and-response-services-2020> 07/06/2021
- 60 Netclean Annual Report; Insight 5: COVID-19 has affected the capacity to investigate child sexual abuse crimes (Netclean, 2021) Accessed from: <https://www.netclean.com/netclean-report-2020/insight-5/> 07/06/2021
- 61 Summary paper on online child sexual exploitation (ECPAT, 2020) Accessed from: <https://www.ecpat.org/wp-content/uploads/2020/12/ECPAT-Summary-paper-on-Online-Child-Sexual-Exploitation-2020.pdf> 22/04/2021
- 62 States divert funds, cut expenditure to foot COVID-19 bill (Economic Times, 2021) Accessed from: <https://economic-times.indiatimes.com/news/india/states-divert-funds-cut-expenditure-to-foot-covid-19-bill/articleshow/82448577.cms?from=mdr> 07/06/2021
- 63 Policy Responses to COVID-19: Iraq (International Monetary Fund, 2021) Accessed from: <https://www.imf.org/en/Topics/imf-and-covid19/Policy-Responses-to-COVID-19#top> 07/06/2021
- 64 UK's drastic cut to overseas aid risks future pandemics, say Sage experts (Guardian, 2021) Accessed from: <https://www.theguardian.com/education/2021/mar/20/uks-drastic-cut-to-overseas-aid-risks-future-pandemics-say-sage-experts> 16/07/2021
- 65 100+ Internet Statistics and Facts for 2021 (Website Hosting Rating, 2021) Accessed from: <https://www.websitehostingrating.com/internet-statistics-facts/> 29/04/2021
- 66 Worldwide digital population as of January 2021 (Statista, 2021) Accessed from: <https://www.statista.com/statistics/617136/digital-population-worldwide/> 29/04/2021
- 67 In-depth analysis of changes in world internet performance (GSMA, 2019) Accessed from: <https://www.gsma.com/membership/resources/in-depth-analysis-of-changes-in-world-internet-performance-using-the-speedtest-global-index/> 29/04/2021
- 68 Number of mobile devices worldwide 2020-2024 (Statista, 2020) Accessed from: <https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/> 29/04/2021
- 69 Children in a digital world (Unicef, 2017) Accessed from: <https://www.unicef.org/media/48601/file> 29/04/2021
- 70 Africa Is the Next Frontier For The Internet (Forbes, 2020) accessed from: <https://www.forbes.com/sites/miri-amtuerk/2020/06/09/africa-is-the-next-frontier-for-the-internet/?sh=e8ecd3b49001> 04/05/2021
- 71 Strong mobile growth predicted for sub-Saharan Africa (Connecting Africa, 2020) Accessed from: http://www.connectingafrica.com/author.asp?section_id=761&doc_id=764310 04/05/2021

- 72 Child Online Safety: Minimising the Risk of Violence, Abuse and Exploitation Online (Broadband Commission, 2019) Accessed from: https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf 02/04/2021
- 73 Mobile technology the key to bringing 'education to all', says UN Broadband Commission (Unesco, 2014) Accessed from: <https://en.unesco.org/news/mobile-technology-key-bringing-education-all-says-broadband-commission> 14/05/2021
- 74 EU Kids Online 2020: Survey Results from 19 Countries (EU Kids Online, 2020) Accessed from: <https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf> 23/02/2021
- 75 The Internet of Toys: Implications of increased connectivity and convergence of physical and digital play in young children (LSE, 2017) Accessed from: <https://blogs.lse.ac.uk/parenting4digitalfuture/2017/07/19/the-internet-of-toys-implications-of-increased-connectivity-and-convergence-of-physical-and-digital-play-in-young-children/> 20/07/2021
- 76 Responding to Online Threats: Minors' Perspectives on Disclosing, Reporting, and Blocking (Thorn, 2021) Accessed from: <https://www.thorn.org/thorn-research-minors-perspectives-on-disclosing-reporting-and-blocking/> 15/07/2021
- 77 Exposure to sexually explicit media in early adolescence (Lin et al., 2020) Accessed from: <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0230242> 16/02/2021
- 78 Growing up in a connected world (UNICEF, 2019) Accessed from: <https://www.unicef-irc.org/publications/pdf/GK0%20Summary%20Report.pdf> 30/04/2021
- 79 Child and adolescent pornography exposure (Hornor, 2020) Accessed from: [https://www.jpedhc.org/article/S0891-5245\(19\)30384-0/fulltext](https://www.jpedhc.org/article/S0891-5245(19)30384-0/fulltext) 30/04/2021
- 80 Working with Children and Young People Who Have Displayed Harmful Sexual Behaviour (Allardyce and Yates, 2020)
- 81 Action to End Child Sexual Abuse and Exploitation (UNICEF, 2020) p.50 Accessed from: <https://www.unicef.org/media/89026/file/CSAE-Report.pdf> 17/05/2021
- 82 EU Kids Online 2020: Survey Results from 19 Countries (EU Kids Online, 2020) Accessed from: <https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf> 23/02/2021
- 83 Growing up in a connected world (UNICEF, 2019) Accessed from: <https://www.unicef-irc.org/publications/pdf/GK0%20Summary%20Report.pdf> 30/04/2021
- 84 Impact of online and offline child sexual abuse: "Everyone deserves to be happy and safe" (NSPCC, 2017) Accessed from: <https://learning.nspcc.org.uk/research-resources/2017/impact-online-offline-child-sexual-abuse> 17/05/2021
- 85 Responding to Online Threats: Minors' Perspectives on Disclosing, Reporting, and Blocking (Thorn, 2021) Accessed from: <https://www.thorn.org/thorn-research-minors-perspectives-on-disclosing-reporting-and-blocking/> 15/07/2021
- 86 How Everyone's Invited's 'rape culture' claims sparked a #MeToo movement in UK schools (Evening Standard, 2021) Accessed from: <https://www.standard.co.uk/insider/everyones-invited-rape-culture-metoo-movement-schools-b925924.html> 18/05/2021
- 87 #MeToo in school: too many children are sexually harassed by classmates (The Guardian, 2018) Accessed from: <https://www.theguardian.com/commentisfree/2018/feb/11/metoo-school-children-teens-sexual-harassment> (18/05/2021)
- 88 Everyone's Invited (Everyone's Invited, 2020) Accessed from: <https://www.everyonesinvited.uk/> 18/05/2021
- 89 Children and parents: Media use and attitudes report 2019 (Ofcom, 2019) Accessed from: https://www.ofcom.org.uk/__data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf 18/05/2021
- 90 PA Consulting Engagement with Edward Dixon (Rigr AI), 18/03/2021
- 91 'End Online Violence: Learnings from Sri Lanka' Conference (End Violence Against Children, 25/02/2021)
- 92 Darknet Cybercrime Threats to South East Asia (UNODC, 2021) Accessed from: https://www.unodc.org/documents/southeastasiaandpacific/Publications/2021/Darknet_Cybercrime_Threats_to_Southeast_Asia_report.pdf 29/04/2021
- 93 PA Consulting engagement with Interpol, 25/03/2021
- 94 Interpol: International police coordination required to combat global cyberthreats (CSO, 2021) Accessed from: <https://www.csoonline.com/article/3624992/interpol-international-police-coordination-required-to-combat-global-cyberthreats.html> 20/07/2021
- 95 Child sexual abuse material: Model legislation and global review (ICMEC, 2021) Accessed from: <https://www.icmec.org/csam-model-legislation/> 29/04/2021
- 96 Falling short: demand side sentencing for online sexual exploitation of children (International Justice Mission, 2020) Accessed from: <https://www.ijmuk.org/images/EMBARGO-8-NOV-20-IJM-REPORT-FALLING-SHORT-Demand-Side-Sentencing-for-Online-Sexual-Exploitation-of-Children.pdf> 15/02/2021
- 97 PA Consulting engagement with Europol, 17/03/2021
- 98 'Legality of Child Pornography' (Wikipedia, 2021) Accessed from: https://en.wikipedia.org/wiki/Legality_of_child_pornography 17/05/2021
- 99 PA Consulting engagement with United States Department of Justice, 22/03/2021

- 100 Safer Technology, Safer Users: The UK as a world-leader in Safety Tech (UK Government, 2020) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/887349/Safer_technology__safer_users-_The_UK_as_a_world-leader_in_Safety_Tech.pdf 18/05/2021
- 101 The UK Safety Tech Sector: 2021 Analysis (DCMS, 2021) Provided by DCMS on 19/05/2021
- 102 The UK Safety Tech Sector: 2021 Analysis (DCMS, 2021) Provided by DCMS on 19/05/2021
- 103 Child Online Safety: Minimising the Risk of Violence, Abuse and Exploitation Online (Broadband Commission, 2019) Accessed from: https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf 2/4/2021
- 104 Child Online Safety: Minimising the Risk of Violence, Abuse and Exploitation Online (Broadband Commission, 2019) Accessed from: https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf 2/4/2021
- 105 Metadata-based detection of child sexual abuse material (Periera, Dodhia and Brown, 2020) Accessed from: <https://arxiv.org/pdf/2010.02387.pdf> 29/04/2021
- 106 PA Consulting engagement with Terre des Hommes, 25/02/2021
- 107 Safer Technology, Safer Users: The UK as a world-leader in Safety Tech (UK Government, 2020) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/887349/Safer_technology__safer_users-_The_UK_as_a_world-leader_in_Safety_Tech.pdf 18/05/2021
- 108 The UK Safety Tech Sector: 2021 Analysis (DCMS, 2021) Provided by DCMS on 19/05/2021
- 109 Together to #ENDviolence: Global Policy Briefing; Key Messages (The End Violence Partnership, 2020) Received via email from the End Violence Partnership on 13/07/2021
- 110 Technology, privacy and rights: keeping children safe from child sexual exploitation and abuse online (WeProtect Global Alliance, 2021) Accessed from: <https://www.weprotect.org/wp-content/uploads/Technology-privacy-and-rights-roundtable-outcomes-briefing.pdf> 02/06/2021
- 111 Handbook for policy makers on the rights of the child in the digital environment (Council of Europe, 2020) Accessed from: <https://rm.coe.int/publication-it-handbook-for-policy-makers-final-eng/1680a069f8> 06/05/2021
- 112 EU Kids Online 2020: Survey Results from 19 Countries (EU Kids Online, 2020) Accessed from: <https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf> 23/02/2021
- 113 Germany's Network Enforcement Act and its impact on social networks (Taylor Wessing, 2018) Accessed from: <https://www.taylorwessing.com/download/article-germany-nfa-impact-social.html> 10/06/21
- 114 Email received from the Office of the e-Safety Commissioner, 13/07/2021
- 115 UK to introduce world first online safety laws (GOV.UK, 2019) Accessed from: <https://www.gov.uk/government/news/uk-to-introduce-world-first-online-safety-laws> 10/06/2021
- 116 The EU unveils its plan to rein in big tech (Economist, 2020) Accessed from: <https://www.economist.com/business/2020/12/15/the-eu-unveils-its-plan-to-rein-in-big-tech> 10/06/2021
- 117 Online Safety and Media Regulation Bill (GOV.IE, 2020) Accessed from: <https://www.gov.ie/en/publication/d8e4c-online-safety-and-media-regulation-bill/> 10/06/2021
- 118 Communication from the Commission to the European parliament, the council, the European economic and Social Committee and the Committee of the Regions: EU Strategy for a more effective fight against child sexual abuse (European Commission, 2020) Accessed from: https://ec.europa.eu/home-affairs/sites/default/files/what-we-do/policies/european-agenda-security/20200724_com-2020-607-commission-communication_en.pdf 10/06/2021
- 119 End-to-End Encryption: Understanding the impacts for child safety online (NSPCC, 2021) Accessed from: <https://www.nspcc.org.uk/globalassets/documents/news/e2ee-pac-report-end-to-end-encryption.pdf> 10/06/2021
- 120 Encryption, Privacy and Children's Right to Protection from Harm (Unicef, 2020) Accessed from: https://www.unicef-irc.org/publications/pdf/Encryption_privacy_and_children%E2%80%99s_right_to_protection_from_harm.pdf 21/07/2021
- 121 Google is testing end-to-end encryption in android messages (Wired, 2020) Accessed from: <https://www.wired.com/story/google-is-testing-end-to-end-encryption-in-android-messages/> 10/06/2021
- 122 NSPCC urges Facebook to stop encryption plans (BBC News, 2020) Accessed from: <https://www.bbc.co.uk/news/technology-51391301> 10/06/2021
- 123 End-to-End Encryption (NSPCC, 2021) Accessed from: <https://www.nspcc.org.uk/globalassets/documents/news/e2ee-pac-report-end-to-end-encryption.pdf> 25/05/2021
- 124 Briefing on the future of digital tools to detect child sexual exploitation and abuse online in Europe (WeProtect Global Alliance, 2021) Accessed from: <https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/600086ba8f-223010c1b4b756/1610647258029/WPGA+European+ePrivacy+briefing+Jan+21.pdf> 10/06/2021
- 125 A battle won, but not the war in the global fight for child safety (NCMEC, 2021) Accessed from: <https://www.missingkids.org/childsafetyfirst#:~:text=As%20NCMEC%20has%20recently%20reported%2C%20we%20have%20seen,to%20offer%20permanent%20solutions%20for%20child%20safety%20online.> 10/06/2021

- 126 Provisional agreement on temporary rules to detect and remove online child abuse (News, European Parliament, 2021) Accessed from: <https://www.europarl.europa.eu/news/en/press-room/20210430IPRO3213/provisional-agreement-on-temporary-rules-to-detect-and-remove-online-child-abuse> 22/06/2021
- 127 Project Beacon: EU comes to political agreement to continue the use of online tools against CSAM (ECPAT, 2021) Accessed from: <https://www.ecpat.org/news/tag/project-beacon/> 21/07/2021
- 128 The EU Strategy on the Rights of the Child and the European Child Guarantee (European Commission, 2021) Accessed from: The EU Strategy on the Rights of the Child and the European Child Guarantee | European Commission (europa.eu) 21/07/2021
- 129 Fighting against child sexual abuse: join the stakeholder consultation (European Commission, 2021) Accessed from: https://ec.europa.eu/home-affairs/news/fighting-against-child-sexual-abuse-join-stakeholder-consultation_en 21/07/2021
- 130 NCMEC's Statement Regarding End-to End Encryption (NCMEC, 2019) Accessed from: <https://www.missingkids.org/blog/2019/post-update/end-to-end-encryption> 10/06/2021
- 131 Encryption, Privacy and Children's Right to Protection from Harm (Unicef, 2020) Accessed from: https://www.unicef-irc.org/publications/pdf/Encryption_privacy_and_children%E2%80%99s_right_to_protection_from_harm.pdf 21/07/2021
- 132 Statement on end-to-end encryption and public safety (Australian Government Department of Home Affairs, 2021) Shared by the Australian Department of Home Affairs by email, 19/05/2021
- 133 VGT position on End-to-End Encryption (Virtual Global Taskforce, 2021) Received via email from the NCA on 14/06/2021
- 134 NCA National Strategic Assessment of Serious and Organised Crime (National Crime Agency, 2021) Received via email from the NCA on 25/05/2021
- 135 PA Consulting Engagement with Dr. Hany Farid, 15/03/2021
- 136 Opinion: Facebook's encryption makes it harder to detect child abuse (Berkeley, 2019) Accessed from: <https://www.ischool.berkeley.edu/news/2019/opinion-facebooks-encryption-makes-it-harder-detect-child-abuse> 10/06/2021
- 137 PA Consulting Engagement with Dr. Hany Farid, 15/03/2021
- 138 PA Consulting Engagement with Dr. Hany Farid, 15/03/2021
- 139 Opinion: Facebook's encryption makes it harder to detect child abuse (Berkeley, 2019) Accessed from: <https://www.ischool.berkeley.edu/news/2019/opinion-facebooks-encryption-makes-it-harder-detect-child-abuse> 10/06/2021
- 140 Encryption, Privacy and Children's Right to Protection from Harm (Unicef, 2020) Accessed from: https://www.unicef-irc.org/publications/pdf/Encryption_privacy_and_children%E2%80%99s_right_to_protection_from_harm.pdf 21/07/2021
- 141 PA Consulting Engagement with Dr. Hany Farid, 15/03/2021
- 142 End-to-End Encryption (NSPCC, 2021) Accessed from: <https://www.nspcc.org.uk/globalassets/documents/news/e2ee-pac-report-end-to-end-encryption.pdf> 25/05/2021
- 143 Encryption, Privacy and Children's Right to Protection from Harm (Unicef, 2020) Accessed from: https://www.unicef-irc.org/publications/pdf/Encryption_privacy_and_children%E2%80%99s_right_to_protection_from_harm.pdf 21/07/2021
- 144 Project Arachnid: Online Availability of Child Sexual Abuse Material (Canadian Centre for Child Protection, 2021) Accessed from: <https://protectchildren.ca/en/resources-research/project-arachnid-csam-online-availability/> 10/06/2021
- 145 Webinar: The Online Harms Bill – more harm than good? (11KBW, 20/05/2021)
- 146 Protection of children should always trump protection of privacy (Julie Inman Grant, eSafety Commissioner, 2020) Accessed from: <https://www.esafety.gov.au/about-us/blog/protecting-children-should-always-trump-protecting-privacy> 10/06/2021
- 147 The Decentralised Web of Hate: White Supremacists are starting to use peer-to-peer technology; are we prepared? (Rebellious Data LLC, 2020) Accessed from: <https://rebellious-data.com/wp-content/uploads/2020/10/P2P-Hate-Report.pdf> 10/06/2021
- 148 Messaging services are providing a more private internet (Economist, 2021) Accessed from: <https://www.economist.com/international/2021/01/23/messaging-services-are-providing-a-more-private-internet> 10/06/2021
- 149 Technology, privacy and rights: keeping children safe from child sexual exploitation and abuse online (WeProtect Global Alliance, 2021) Accessed from: <https://www.weprotect.org/wp-content/uploads/Technology-privacy-and-rights-roundtable-outcomes-briefing.pdf> 02/06/2021
- 150 Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse (WeProtect Global Alliance, 2020) Accessed from: <https://www.weprotect.org/library/voluntary-principles-to-counter-online-child-sexual-exploitation-and-abuse/> 10/06/2021
- 151 Tech giants list principles for handling harmful content (Axios, 2021) Accessed from: <https://www.axios.com/tech-giants-list-principles-for-handling-harmful-content-5c9cfba9-05bc-49ad-846a-baf01abf5976.html> 10/06/2021
- 152 The Technology Coalition Announces Project Protect (Technology Coalition, 2020) Accessed from: <https://www.technology-coalition.org/2020/05/28/a-plan-to-combat-online-child-sexual-abuse/> 24/06/2021

- 153 Online enticement reports skyrocket in 2020 (NCMEC, 2021) Accessed from: <https://www.missingkids.org/blog/2021/online-enticement-reports-skyrocket-in-2020> 24/02/2021
- 154 Online enticement (NCMEC) Accessed from: <https://www.missingkids.org/netsmartz/topics/onlineenticement> 19/04/2021
- 155 Online child sexual abuse activity has increased (NetClean, 2021) Accessed from: <https://www.netclean.com/net-clean-report-2020/insight-2/> 26/01/2021
- 156 Trends identified in CyberTipline sextortion reports (NetClean, 2016) Accessed from: <https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/sextortionfactsheet.pdf> 01/03/2021
- 157 Child Online Safety: Minimising the Risk of Violence, Abuse and Exploitation Online (Broadband Commission, 2019) Accessed from: https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf 02/04/2021
- 158 Out of the Shadows (Economist Impact, 2018) Accessed from: <https://outoftheshadows.eiu.com/> 25/01/2021
- 159 Online grooming of children for sexual purposes (ICMEC, 2017) Accessed from: https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf 04/02/2021
- 160 Kids & Tech: Evolution of Today's Digital Natives (Influence Central, 2017) Accessed from: <https://influence-central.com/trendspotting/launching-the-new-influence-central-trend-report> 12/04/2021
- 161 Technology working group report (Child Dignity Foundation, 2018) Accessed from: <https://johnc1912.files.wordpress.com/2018/11/1d5b1-cdatechnicalworkinggroupreport.pdf> 26/02/2021
- 162 EU Kids Online 2020: Survey Results from 19 Countries (EU Kids Online, 2020) Accessed from: <https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf> 23/02/2021
- 163 Online grooming: What it is, how it happens, and how to defend children (Thorn, 2020) Accessed from: <https://www.thorn.org/blog/online-grooming-what-it-is-how-it-happens-and-how-to-defend-children/> 07/04/2021
- 164 The impact of the Coronavirus pandemic on child welfare: Online abuse (NSPCC, 2020) Accessed from: <https://learning.nspcc.org.uk/media/2390/impact-of-coronavirus-pandemic-on-child-welfare-online-abuse.pdf> 10/03/2021
- 165 Trends identified in cyberipline sextortion reports (NetClean, 2016) Accessed from: <https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/sextortionfactsheet.pdf> 01/03/2021
- 166 The impact of the Coronavirus pandemic on child welfare: Online abuse (NSPCC, 2020) Accessed from: <https://learning.nspcc.org.uk/media/2390/impact-of-coronavirus-pandemic-on-child-welfare-online-abuse.pdf> 11/03/2021
- 167 COVID-19: Child Sexual Exploitation (Europol, 2020) Accessed from: <https://www.europol.europa.eu/covid-19/covid-19-child-sexual-exploitation> 28/01/2021
- 168 COVID-19 accelerates global video gaming market to \$170bn (Consultancy-me.com, 2020) Accessed from: <https://www.consultancy-me.com/news/3041/covid-19-accelerates-global-gaming-market-to-170-billion> 16/02/2021
- 169 The Marie Collins Foundation, Accessed from: <https://www.mariecollinsfoundation.org.uk/> 29/04/2021
- 170 Survey of Technology Companies (WeProtect Global Alliance and Technology Coalition, 2021) See Annex A: Findings from WeProtect Global Alliance/Technology Coalition Survey of Technology Companies
- 171 Online grooming of children for sexual purposes (ICMEC, 2017) Accessed from: https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf 04/02/2021
- 172 Safety-by-design overview (eSafety Commissioner, 2019) Accessed from: <https://www.esafety.gov.au/sites/default/files/2019-10/SBD%20-%20Overview%20May19.pdf> 11/02/2021
- 173 Digital Age Assurance Tools and Children's Rights Online across the Globe (UNICEF, 2021) Accessed from: <https://www.unicef.org/media/97461/file/Digital%20Age%20Assurance%20Tools%20and%20Children%E2%80%99s%20Rights%20Online%20across%20the%20Globe.pdf> 07/05/2021
- 174 Video games and online chats are 'hunting grounds' for sexual predators (New York Times, 2019) Accessed from: <https://www.nytimes.com/interactive/2019/12/07/us/video-games-child-sex-abuse.html> 21/04/2021
- 175 Case study submission from TikTok, received on 10/05/2021
- 176 Continuing to Make Instagram Safer for the Youngest Members of Our Community (Instagram, 2021) Accessed from: <https://about.instagram.com/blog/announcements/continuing-to-make-instagram-safer-for-the-youngest-members-of-our-community> 21/04/2021
- 177 What is a supervised experience on YouTube? (Google, 2021) Accessed from: <https://support.google.com/youtube/answer/10314940?hl=en> 20/07/2021
- 178 Perpetrators of sexual violence: statistics (RAINN) Accessed from: <https://www.rainn.org/statistics/perpetrators-sexual-violence> 16/04/2021
- 179 The sexual exploitation and abuse of deaf and disabled children online (WeProtect Global Alliance, 2021) Accessed from: <https://www.weprotect.org/wp-content/uploads/Intelligence-briefing-2021-The-sexual-exploitation-and-abuse-of-disabled-children.pdf> 23/02/2021

- 180 Ending violence against children: key messages and statistics (End Violence Against Children) [https://www.end-violence.org/sites/default/files/paragraphs/download/Key Messages_Long_O.pdf](https://www.end-violence.org/sites/default/files/paragraphs/download/Key_Messages_Long_O.pdf) 12/04/2021
- 181 CyberTipline: 2019 & 2020 Reports by country (NCMEC, 2020) accessed from: <https://www.missingkids.org/gethelp-now/cybertipline> 19/04/2021
- 182 Online sexual exploitation of children in the Philippines (International Justice Mission, 2020) Accessed from: https://www.ijm.org/documents/studies/Final-Public-Full-Report-5_20_2020.pdf 17/02/2021
- 183 Annual Report 2020 (INHOPE, 2021) Accessed from: <https://inhope.org/media/pages/the-facts/download-our-whitepapers/c16bc4d839-1620144551/inhope-annual-report-2020.pdf> 06/05/2021
- 184 IWF Annual Report: International Overview (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/overview> 21/04/2021
- 185 Self-generated child sexual abuse (IWF Annual Report, 2020) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/selfgenerated> 29/07/2021
- 186 Impact of coronavirus disease on different manifestations of sale and sexual exploitation of children (United Nations, 2021) Accessed from: https://reliefweb.int/sites/reliefweb.int/files/resources/A_HRC_46_31_E.pdf 04/03/2021
- 187 Violencia sexual a menores ya deja mas de mil victimas en lo corrido de 2021 (LAFM, 2021) Accessed from: <https://www.lafm.com.co/colombia/violencia-sexual-menores-ya-deja-mas-de-mil-victimas-en-lo-corrido-de-2021> 11/03/2021
- 188 Abuso sexual en internet y redes de trata (Infobae, 2020) Accessed from: <https://www.infobae.com/america/mexico/2020/07/27/abuso-sexual-en-internet-y-redes-de-trata-los-crimenes-contra-la-ninez-que-aumentaron-durante-la-pandemia/> 25/02/2021
- 189 Production and distribution of child sexual abuse material by parental figures (Australian Institute of Criminology, 2021) Accessed from: https://www.aic.gov.au/sites/default/files/2021-02/ti616_production_and_distribution_of_child_sexual_abuse_material_by_parental_figures.pdf 09/03/2021
- 190 Los casos de abuso sexual contra menores en espana se multiplican por 4 en la ultima decada (Levante, 2021) Accessed from: <https://protect-eu.mimecast.com/s/WuEPCWn-WgFxLBY3Hxchqm?domain=levante-emv.com> 23/02/2021
- 191 Production and distribution of child sexual abuse material by parental figures (Australian Institute of Criminology, 2021) Accessed from: https://www.aic.gov.au/sites/default/files/2021-02/ti616_production_and_distribution_of_child_sexual_abuse_material_by_parental_figures.pdf 09/03/2021
- 192 Online enticement of children: an in-depth analysis of CyberTipline reports (National Center for Missing and Exploited Children, 2017) Accessed from: <https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/Online%20Enticement%20Pre-Travel1.pdf> 11/02/2021
- 193 The cycle of child sexual abuse stops now (Project Arachnid) Accessed from: <https://projectarachnid.ca/en/07/04/2021>
- 194 PA Consulting engagement with United States Department of Justice, 22/03/2021
- 195 PA Consulting engagement with United Kingdom National Crime Agency, 18/02/2021
- 196 Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic (Europol, 2020) Accessed from: <https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic> 26/01/2021
- 197 Child abuse predator 'handbook' lists ways to target children during coronavirus lockdown (The Guardian, 2020) Accessed from: <https://www.theguardian.com/society/2020/may/14/child-abuse-predator-handbook-lists-ways-to-target-children-during-coronavirus-lockdown> 23/02/2021
- 198 Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic (Europol, 2020) Accessed from: <https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic> 26/01/2021
- 199 PA Consulting engagement with Australian Centre to Counter Child Exploitation, 01/03/2021
- 200 South Korea confronts its voyeurism epidemic (The Guardian, 2018) Accessed from: <https://www.theguardian.com/world/2018/jul/03/a-part-of-daily-life-south-korea-confronts-its-voyeurism-epidemic-sexual-harassment> 08/03/2021
- 201 Netclean Report 2019: A report about child sexual abuse crime (Netclean, 2019) Accessed from: <https://www.netclean.com/netclean-report-2019/> 28/01/2021
- 202 A deepfake porn bot is being used to abuse thousands of women (WIRED, 2020) Accessed from: <https://www.wired.co.uk/article/telegram-deepfakes-deepnude-ai> 19/03/2021
- 203 Cybersex, erotic tech and virtual intimacy are on the rise during COVID-19 (The Conversation, 2020) Accessed from: <https://theconversation.com/cybersex-erotic-tech-and-virtual-intimacy-are-on-the-rise-during-covid-19-141769> 19/03/2021
- 204 Immersive Technologies – Position Statement (e-Safety Commissioner, 2021) Accessed from: <https://www.esafety.gov.au/about-us/tech-trends-and-challenges/immersive-tech> 14/07/2021
- 205 CGI (Computer Generated Imagery) (TechTarget, 2016) Accessed from: <https://whatis.techtarget.com/definition/CGI-computer-generated-imagery> 08/04/2021
- 206 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Interagency Working Group on Sexual Exploitation of Children, 2016) Accessed from: https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines_en.pdf 17/03/2021

- 207 What is deepfake? (Business Insider, 2021) Accessed from: <https://www.businessinsider.com/what-is-deep-fake?r=US&IR=T#:~:text=Recently%2C%20deepfake%20technology%20has%20been,with%20another%20in%20re-corded%20video> 08/04/2021
- 208 PA Consulting engagement with Terre des Hommes, 25/02/2021
- 209 Online child sexual abuse and exploitation: Current forms and good practice for prevention and protection (ECPAT France, 2017) Accessed from: https://ecpat-france.fr/wp-content/uploads/2018/10/Revue-OCSE_ANG-min.pdf 09/08/2021
- 210 Non-photographic visual depictions (Internet Watch Foundation, 2007) Accessed from: <https://www.iwf.org.uk/what-we-do/who-we-are/consultations/non-photographic-visual-depic-tions> 17/03/2021
- 211 Child Sexual Abuse Material: Model Legislation and Global Review (International Center for Missing and Exploited Children, 2018) Accessed from: <https://www.icmec.org/wp-content/uploads/2018/12/CSAM-Model-Law-9th-Ed-FINAL-12-3-18.pdf> 05/03/2021
- 212 Computer-generated 'Sweetie' catches online predators (BBC News, 2013) Accessed from: <https://www.bbc.co.uk/news/uk-24818769> 08/03/2021
- 213 Child sexual abuse in the digital era: Rethinking legal frameworks and transnational law enforcement collaboration (Universiteit Leiden, 2020) Accessed from: <https://scholarly-publications.universiteitleiden.nl/access/item%3A2966712/view> 07/05/2021
- 214 National Strategic Assessment of Serious and Organised Crime 2020 (National Crime Agency, 2020) Accessed from: <https://www.nationalcrimeagency.gov.uk/news/nsa2020> 24/03/2021
- 215 Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic (Europol, 2020) Accessed from: <https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-vic-tims-of-online-child-sexual-abuse-during-covid-19-pandemic> 26/01/2021
- 216 PA Consulting engagement with Interpol, 25/03/2021
- 217 PA Consulting engagement with Ethel Quayle, 04/03/2021
- 218 The Internet: Investigation Report (Independent Inquiry into Child Sexual Exploitation and Abuse, 2020) Accessed from: <https://www.iicsa.org.uk/publications/investigation/internet> 02/02/2021
- 219 Internet Organised Crime Threat Assessment (IOCTA) 2020 (Europol, 2020) Accessed from: <https://www.europol.europa.eu/activities-services/main-reports/internet-organ-ised-crime-threat-assessment-iocta-2020> 30/03/2021
- 220 Europol Serious and Organised Crime Threat Assessment (SOCTA) 2021 (Europol, 2021) Accessed from: <https://www.europol.europa.eu/activities-services/main-reports/euro-pean-union-serious-and-organised-crime-threat-assessment> 20/04/2021
- 221 Child Rescue Coalition (CRC): Protecting Innocence Through Technology (CRC, 2021) Email received from CRC, 30/03/2021
- 222 Global Threat Assessment 2019 (WeProtect Global Alliance, 2019) Accessed from: <https://www.weprotect.org/issue/global-threat-assessment/> 26/01/2021
- 223 Hackers leaked 22 million records on the dark web in 2020 (ID Agent, 2020) Accessed from: <https://www.idagent.com/hackers-leaked-22-million-records-on-the-dark-web-in-2020> 29/04/2021
- 224 Trends in Online Child Sexual Abuse Material (ECPAT, 2017) Accessed from: <https://www.ecpat.org/wp-content/up-loads/2016/05/Emerging-Issues-and-Global-Threats-Child-ren-online-2017-1.pdf> 25/03/2021
- 225 COVID-19: Child Sexual Exploitation (Europol, 2020) Ac-cessed from: <https://www.europol.europa.eu/covid-19/cov-id-19-child-sexual-exploitation> 20/04/2021
- 226 Brave.com now has its own Tor onion service, providing more users with secure access to Brave (Brave.com, 2020) Accessed from: <https://brave.com/new-onion-service/> 20/04/20
- 227 Tor (Investopedia, 2019) Accessed from: <https://www.investo-pedia.com/terms/t/tor.asp> 07/05/2021
- 228 PA Consulting engagement with United States Department of Justice, 07/04/2021 NCMEC Engagement
- 229 PA Consulting engagement with United Kingdom National Crime Agency, 18/02/2021
- 230 PA Consulting engagement with United States National Centre for Missing and Exploited Children, 16/03/2021
- 231 Millions of attempts to access child sexual abuse online during lockdown (Internet Watch Foundation, 2020) Accessed from: <https://www.iwf.org.uk/news/millions-of-attempts-to-access-child-sexual-abuse-online-during-lockdown> 08/02/2021
- 232 COVID-19 conversations: The Crisis of Online Child Exploita-tion (Equality Now, 2021) Accessed from: https://www.equali-tynow.org/covid_19_online_exploitation 07/06/2021
- 233 Impact of coronavirus disease on different manifestations of sale and sexual exploitation of children (United Nations, 2021) Accessed from: https://reliefweb.int/sites/reliefweb.int/files/resources/A_HRC_46_31_E.pdf 04/03/2021
- 234 The Motivation-Facilitation Model of Sexual Offending (Michael C. Seto, 2017) Accessed from: <https://journals.sagepub.com/doi/full/10.1177/1079063217720919> 29/07/2021
- 235 Internet Sex Offenders (Seto, Michael C., 2013)
- 236 Falling short: demand side sentencing for online sexual exploitation of children (International Justice Mission, 2020) Accessed from: <https://www.ijmuk.org/images/EMBAR-GO-8-NOV-20-IJM-REPORT-FALLING-SHORT-Demand-Side-Sentencing-for-Online-Sexual-Exploitation-of-Children.pdf> 15/02/2021

- 237 Sexual interests of child sexual exploitation material (CSEM) consumers (Fortin and Proulx, 2018) Accessed from: <https://journals.sagepub.com/doi/10.1177/0306624X1879413511/02/2021>
- 238 Prevention, disruption and deterrence of online child sexual exploitation and abuse (Quayle, 2020) Accessed from: <https://www.research.ed.ac.uk/en/publications/prevention-disruption-and-deterrence-of-online-child-sexual-explo> 05/03/2021
- 239 How extreme porn has become a gateway drug into child abuse (The Guardian, 2020) Accessed from: <https://www.theguardian.com/global-development/2020/dec/15/how-extreme-porn-has-become-a-gateway-drug-into-child-abuse> 15/02/2021
- 240 Effects of automated messages on internet users attempting to access 'barely legal' pornography (Prichard, Wortley, Waters, Spiranovic, Hunn, Krone, 2020) Received from Donald Findlater (Lucy Faithfull Foundation), 16/02/2021
- 241 Exposure to sexually explicit media in early adolescence (Lin et al., 2020) Accessed from: <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0230242> 16/02/2021
- 242 Working with Children and Young People Who Have Displayed Harmful Sexual Behaviour (Allardyce and Yates, 2020)
- 243 On Youtube's Digital Playground, an Open Gate for Pedophiles (The New York Times, 2019) Accessed from: <https://www.nytimes.com/2019/06/03/world/americas/youtube-pedophiles.html?module=inline> 04/03/2021
- 244 Prevention, disruption and deterrence of online child sexual exploitation and abuse (Quayle, 2020) Accessed from: <https://www.research.ed.ac.uk/en/publications/prevention-disruption-and-deterrence-of-online-child-sexual-explo> 05/03/2021
- 245 On Youtube, a network of paedophiles is hiding in plain sight (WIRED, 2019) Accessed from: <https://www.wired.co.uk/article/youtube-pedophile-videos-advertising> 31/03/2021
- 246 Barriers Abusers Overcome In Order To Abuse (Psychology Tools) Accessed from: <https://www.psychologytools.com/resource/barriers-abusers-overcome-in-order-to-abuse/> 29/03/2021
- 247 Child Sexual Abuse (Finkelhor, 1984)
- 248 The Four Rs of Responsibility, Part 1: Removing Harmful Content (Youtube, 2019) Accessed from: <https://blog.youtube/inside-youtube/the-four-rs-of-responsibility-remove/> 27/07/2021
- 249 Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation (NatCen Social Research, 2017) Accessed from: <https://natcen.ac.uk/media/1535277/Behaviours-and-characteristics-of-perpetrators-of-online-facilitated-child-sexual-abuse-and-exploitation.pdf> 09/02/2021
- 250 Survey of Technology Companies (WeProtect Global Alliance and Technology Coalition, 2021) See Annex A: Findings from WeProtect Global Alliance/Technology Coalition Survey of Technology Companies
- 251 Online sexual exploitation of children in the Philippines (International Justice Mission, 2020) Accessed from: https://www.ijm.org/documents/studies/Final-Public-Full-Report-5_20_2020.pdf 23/02/2021
- 252 Effects of automated messages on internet users attempting to access 'barely legal' pornography (Pritchard et al., 2020)
- 253 Prevention, disruption and deterrence of online child sexual exploitation and abuse (Quayle, 2020) Accessed from: <https://www.research.ed.ac.uk/en/publications/prevention-disruption-and-deterrence-of-online-child-sexual-explo> 05/03/2021
- 254 Ground-breaking research on perpetrator prevention (Oak Foundation, 2021) Accessed from: <https://oakfnd.org/groundbreaking-research-on-perpetration-prevention/> 13/07/2021
- 255 IWF Annual Report: About Our Year (IWF, 2020) Accessed from: <https://annualreport2020.iwf.org.uk/about/year/ceo> 21/04/2021
- 256 Game-changing chatbot to target people trying to access child sexual abuse online (IWF, 2020) Accessed from: <https://www.iwf.org.uk/news/game-changing%E2%80%99-chatbot-to-target-people-trying-to-access-child-sexual-abuse-online> 20/04/2021
- 257 Prevention, disruption and deterrence of online child sexual exploitation and abuse (Quayle, 2020) Accessed from: <https://www.research.ed.ac.uk/en/publications/prevention-disruption-and-deterrence-of-online-child-sexual-explo> 05/03/2021
- 258 Suojellaan Lapsia, Accessed from: <https://suojellaanlapsia.fi/> 29/04/2021
- 259 COVID-19 and Missing and Exploited Children (NCMEC, 2021) Accessed from: <https://www.missingkids.org/blog/2020/covid-19-and-missing-and-exploited-children> 22/04).
- 260 IWF Annual Report: 2020 Trends and Data (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends> 22/04/2021
- 261 Annual Report 2020 (INHOPE, 2021) Accessed from: <https://inhope.org/media/pages/the-facts/download-our-whitepapers/c16bc4d839-1620144551/inhope-annual-report-2020.pdf> 06/05/2021
- 262 PA Consulting engagement with NCMEC, 16/03/2021
- 263 PA Consulting Engagement with NCMEC, 22/04/2021
- 264 IWF Annual Report: Site types analysis (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/sitetypes> 22/04/2021

- 265 COVID-19: Child Sexual Exploitation (Europol, 2020) Accessed from: <https://www.europol.europa.eu/covid-19/covid-19-child-sexual-exploitation> 28/01/2021
- 266 PA Consulting engagement with Interpol, 25/03/2021
- 267 IWF Annual Report: Hidden Services (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/Trends/International/Other/Hidden> 22/04
- 268 IWF Annual Report: Glossary (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/glossary> 10/05/2021
- 269 How child sexual abuse material is stored (Netclean, 2019) Accessed from: <https://www.netclean.com/netclean-report-2019/insight-4/> 22/04/2021
- 270 Annual Report 2020 (INHOPE, 2021) Accessed from: <https://inhope.org/media/pages/the-facts/download-our-whitepapers/c16bc4d839-1620144551/inhope-annual-report-2020.pdf> 06/05/2021
- 271 PA Consulting engagement with Edward Dixon (Rigr AI), 18/03/2021
- 272 PA Consulting engagement with United States Department of Justice, 22/03/2021
- 273 PA Consulting engagement with Edward Dixon (Rigr AI), 18/03/2021
- 274 Preventing Child Exploitation on our Apps (Facebook, 2020) Accessed from: <https://about.fb.com/news/2021/02/preventing-child-exploitation-on-our-apps/#:~:text=Using%20our%20apps%20to%20harm,authorities%20to%20keep%20children%20safe.> 22/04/2021
- 275 Production and Active Trading of Child Sexual Exploitation Images Depicting Identified Victims (Thorn, 2018) Accessed from: https://www.missingkids.org/content/dam/missing-kids/pdfs/ncmec-analysis/Production%20and%20Active%20Trading%20of%20CSAM_FullReport_FINAL.pdf 15/07/2021
- 276 Study on the effects of new information technologies on the abuse and exploitation of children (United Nations Office on Drugs and Crime, 2015) Accessed from: https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf 22/04/2021
- 277 Crime investigations of 'child abuse material' - Challenges and opportunities posed by digital technology (Marie Eneman, 2020) Accessed from: https://www.researchgate.net/publication/344072738_Crime_investigations_of_'child_abuse_material'_-_Challenges_and_opportunities_posed_by_digital_technology 10/05/2021
- 278 Production of child sexual abuse material by parental figures (Australian Government, Institute of Criminology, 2021) Accessed from: https://www.aic.gov.au/sites/default/files/2021-02/ti616_production_and_distribution_of_child_sexual_abuse_material_by_parental_figures.pdf 16/07/2021
- 279 Understanding the intentions of Child Sexual Abuse Material (CSAM) sharers (Facebook Research, 2021) Accessed from: <https://research.fb.com/blog/2021/02/understanding-the-intentions-of-child-sexual-abuse-material-csam-sharers/> 29/06/2021
- 280 IWF Annual Report: Commercial content (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/Trends/International/Commercial> 22/04/2021
- 281 IWF Annual Report: Domain analysis (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/domain> 22/04/2021
- 282 IWF Annual Report: Commercial content (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/Trends/International/Commercial> 22/04/2021
- 283 Cryptocurrency and the trade of online child sexual abuse material (ICMEC, 2021) Accessed from: https://cdn.icmec.org/wp-content/uploads/2021/03/Cryptocurrency-and-the-Trade-of-Online-Child-Sexual-Abuse-Material_03.17.21-publish-1.pdf 22/04/21
- 284 IWF Annual Report: Other Trends (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/other> 22/04/2021
- 285 IWF Annual Report: Other Trends (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/other> 22/04/2021
- 286 IWF Annual Report: Other Trends (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/other> 22/04/2021
- 287 Hash Values: Fingerprinting Child Sexual Abuse Material (NetClean, 2018) Accessed from: <https://www.netclean.com/2018/10/30/hash-values/> 22/04/2021
- 288 International Child Sexual Exploitation Database (INTERPOL, 2018) Accessed from: <https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database> 22/04/2021
- 289 IWF Annual Report: Hidden Services (IWF, 2020) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/other/hidden> 10/05/2021
- 290 IWF Annual Report: Geographical hosting (IWF, 2020) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/geographic> 10/05/2021
- 291 Survey of Technology Companies (WeProtect Global Alliance and Technology Coalition, 2021) See Annex A: Findings from WeProtect Global Alliance/Technology Coalition Survey of Technology Companies
- 292 PA Consulting engagement with IWF, 01/03/2021
- 293 PA Consulting engagement with Interpol, 25/03/2021
- 294 PA Consulting engagement with IWF, 01/03/2021
- 295 Technology working group report (Child Dignity Foundation, 2018) Accessed from: <https://johnc1912.files.wordpress.com/2018/11/1d5b1-cdatechnicalworkinggroupreport.pdf> 26/02/2021
- 296 Child Dignity Alliance: Technical Working Group Report (Child Dignity Alliance, 2017) Accessed from: <https://static1.squarespace.com/static/5a4d5d4e7131a5845cd690c/t/5c17cdf4032be42f613e28e4/1545063925977/Child+safety+Report+vD+for+web.pdf> 22/04/2021

- 297 PA Consulting engagement with Edward Dixon (Rigr AI), 18/03/2021
- 298 IWF Annual Report: Self-generated content study (IWF, 2012) Accessed from: <https://www.iwf.org.uk/sites/default/files/reports/2016-02/IWF%202012%20Annual%20and%20Charity%20Report%20%28web%29.pdf> 06/05/2021
- 299 Online child sexual abuse and exploitation: Current forms and good practice for prevention and protection (ECPAT, 2017) Accessed from: https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE_ANG-min.pdf 22/04/2021
- 300 IWF Annual Report: Self-generated child sexual abuse (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/selfgenerated> 06/05/2021
- 301 PA Consulting engagement with Internet Watch Foundation, 01/03/2021
- 302 Interim code of practice on online child sexual exploitation and abuse (accessible version)(GOV.UK, 2020) Accessed from: <https://www.gov.uk/government/publications/online-harms-interim-codes-of-practice/interim-code-of-practice-on-online-child-sexual-exploitation-and-abuse-accessible-version> 19/07/2021
- 303 Initial Situational Analysis on Online Child Sexual Exploitation in Cambodia (Royal Government of Cambodia, 2019) Accessed from: https://aplecambodia.org/wp-content/uploads/2020/04/Research-on-Online-Child-Sexual-Exploitation-in-Cambodia_ENG.pdf 06/05/2021
- 304 Prevalence of Multiple Forms of Sexting Behaviour Among Youth (Madigan et al., 2018) Accessed from: <https://jamanetwork.com/journals/jamapediatrics/fullarticle/2673719?resultClick=1> 06/05/2021
- 305 'Staying Safe Online' survey: wat unwanted sexual images are being sent to teenagers on social media? (University College London, 2019) Accessed from: <https://blogs.ucl.ac.uk/ioe/2020/06/19/staying-safe-online-survey-what-unwanted-sexual-images-are-being-sent-to-teenagers-on-social-media/> 20/07/2021
- 306 PA Consulting engagement with United Kingdom National Crime Agency, 18/02/2021
- 307 IWF Annual Report: Who we are (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/about/us> 11/05/2021
- 308 IWF Annual Report: Self-generated child sexual abuse (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/selfgenerated> 06/05/2021
- 309 An Exploratory Study of Sexting Behaviours Among Heterosexual and Sexual Minority Early Adolescents (Van Ouytsel et al., 2019) Accessed from: <https://pubmed.ncbi.nlm.nih.gov/31473082/> 14/05/2021
- 310 Look at me: Teens, Sexting, and Risks (Internet Matters, 2021) Accessed from <https://www.internetmatters.org/wp-content/uploads/2020/06/Internet-Matters-Look-At-Me-Report-1.pdf> 06/05/2021
- 311 Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation (National Centre for Social Research, 2018) Accessed from: <https://www.iicsa.org.uk/key-documents/3720/download/rapid-evidence-assessment-behaviour-characteristics-perpetrators-online-facilitated-child-sexual-abuse-exploitation.pdf> 06/05/2021
- 312 Online harmful sexual behaviours in children and young people under 18 (eSafety Commissioner, 2020) Accessed from: <https://www.esafety.gov.au/sites/default/files/2020-09/Online%20harmful%20sexual%20behaviours%20Position%20statement.pdf> 13/07/2021
- 313 IWF Annual Report: Self-generated child sexual abuse (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/selfgenerated> 06/05/2021
- 314 Self-Generated Child Sexual Abuse Material: Attitudes and Experiences (Thorn, 2019) Accessed from: https://info.thorn.org/hubfs/Research/08112020_SG-CSAM_AttitudesExperiences-Report_2019.pdf 28/07/2021
- 315 A quantitative and qualitative examination of the impact of online pornography on the values, attitudes, beliefs and behaviours of children and young people (NSPCC, Children's Commissioner, Middlesex University London, 2016) Accessed from: <https://www.childrenscommissioner.gov.uk/wp-content/uploads/2017/06/MDX-NSPCC-OCC-Online-Pornography-Report.pdf> 28/07/2021
- 316 A Rapid Assessment of Live Streaming of Online Sexual Abuse and Exploitation of Children and Young People in Kathmandu (ECPAT Luxembourg, ChildSafeNet) Draft, due to be published in 2021. Received by email from ChildSafeNet Nepal, 04/03/2021
- 317 EU Kids Online 2020: Survey Results from 19 Countries (EU Kids Online, 2020) Accessed from: <https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf> 23/02/2021
- 318 Online Nation: 2021 Report (Ofcom, 2021) Accessed from: https://www.ofcom.org.uk/__data/assets/pdf_file/0013/220414/online-nation-2021-report.pdf 24/06/2021
- 319 Faster Takedown of Online Sexual Abuse Sought (Manila-Standard.Net, 2021) Accessed from: <https://manilastandard.net/mobile/article/349129> 06/05/2021
- 320 Initial Situational Analysis on Online Child Sexual Exploitation in Cambodia (Royal Government of Cambodia, 2019) Accessed from: https://aplecambodia.org/wp-content/uploads/2020/04/Research-on-Online-Child-Sexual-Exploitation-in-Cambodia_ENG.pdf 06/05/2021
- 321 The children selling explicit videos on OnlyFans (BBC News, 2021) Accessed from: <https://www.bbc.co.uk/news/uk-57255983> 07/07/2021
- 322 Netclean Annual Report 2020; Insight 4: Moderate increase in actual investigations and cases (Netclean, 2020) Accessed from: <https://www.netclean.com/netclean-report-2020/insight-4/> 06/05/2021

- 323 'Grave threat' to children from predatory internet groomers as online child sexual abuse material soars to record levels (IWF, 2021) Accessed from: <https://www.iwf.org.uk/news/%E2%80%98grave-threat%E2%80%99-children-predatory-internet-groomers-online-child-sexual-abuse-material-soars> 07/05/2021
- 324 Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation (National Centre for Social Research, 2018) Accessed from: <https://www.iicsa.org.uk/key-documents/3720/download/rapid-evidence-assessment-behaviour-characteristics-perpetrators-online-facilitated-child-sexual-abuse-exploitation.pdf> 06/05/2021
- 325 Emerging Patterns and Trends Report: Online-Produced Sexual Content (IWF, 2015) p.3 Accessed from: https://www.iwf.org.uk/sites/default/files/inline-files/Online-produced_sexual_content_report_100315.pdf 19/05/2021
- 326 Self-Generated Child Sexual Abuse Material: Attitudes and Experiences (Thorn, 2019) Accessed from: https://f.hubspotusercontent00.net/hubfs/7145355/Research/08112020_SG-CSAM_AttitudesExperiences-Report_2019.pdf?__hstc=208625165.851aa734d938b21fee07aa6d05-bc9e7.1604505256798.1614622415296.1614700924025.7&__hssc=208625165.2.1614700924025&__hsfp=723267087 06/05/2021
- 327 The Internet: Investigation Report (Independent Inquiry into Child Sexual Exploitation and Abuse, 2020) Accessed from: <https://www.iicsa.org.uk/publications/investigation/internet> 02/02/2021
- 328 EU Kids Online 2020: Survey Results from 19 Countries (EU Kids Online, 2020) Accessed from: <https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf> 23/02/2021
- 329 PA Consulting Engagement with SafeBAE, 02/03
- 330 SafeToNet acquires German mobile phone stores to safeguard children online (PR Newswire, 2021) Accessed from: <https://www.prnewswire.com/news-releases/safetonet-acquires-german-mobile-phone-stores-to-safeguard-children-online-301247334.html> 14/05/2021
- 331 Handbook for policy makers on the rights of the child in the digital environment (Council of Europe, 2020) Accessed from: <https://www.coe.int/t/t09/Document/Handbook%20for%20policy%20makers%20on%20the%20rights%20of%20the%20child%20in%20the%20digital%20environment.pdf> 06/05/2021
- 332 Teen sexting is decriminalised between partners of similar age (news.com.au, 2018) Accessed from: <https://www.news.com.au/national/nsw-act/courts-law/teen-sexting-is-decriminalised-between-partners-of-similar-age/news-story/3fdceb4adb2c6028eab1f76a86ba5ab> 06/05/2021
- 333 Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse (Council of Europe, 2007) Accessed from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/699615/MS4.2018_Lanzarote_CM9602_WEB.pdf 22/06/2021
- 334 Police Response to Youth Offending Around the Generation and Distribution of Indecent Images of Children and its Implications (University of Suffolk/ Marie Collins Foundation, 2019) Accessed from: https://www.uos.ac.uk/sites/www.uos.ac.uk/files/FOI-Report-Final-Outcome-21_2.pdf 13/05/2021
- 335 Sharing nudes and semi-nudes: advice for education settings working with children and young people (GOV.UK, 2020) Accessed from: <https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people> 01/06/2021
- 336 Action to end Child Sexual Abuse and Exploitation (UNICEF/ End Violence Against Children, 2020) Accessed from <https://www.unicef.org/media/89206/file/CSAE-Brief-v3.pdf> 13/05/2021
- 337 Action to end Child Sexual Abuse and Exploitation (UNICEF/ End Violence Against Children, 2020) Accessed from <https://www.unicef.org/media/89206/file/CSAE-Brief-v3.pdf> 13/05/2021
- 338 Action to end Child Sexual Abuse and Exploitation (UNICEF/ End Violence Against Children, 2020) Accessed from <https://www.unicef.org/media/89206/file/CSAE-Brief-v3.pdf> 13/05/2021
- 339 Sexting among high school students in a metropolis in Ghana: an exploratory study (Baiden et al., 2019) Accessed from: <https://www.tandfonline.com/doi/abs/10.1080/17482798.2020.1719854> 07/05/2021
- 340 Sexting: Prevalence, Predictors, and Associated Sexual Risk Behaviors among Postsecondary School Young People in Ibadan, Nigeria (Olatunde and Balogun, 2017) Accessed from: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5420550/> 07/05/2021
- 341 Self-Generated Child Sexual Abuse Material: Attitudes and Experiences (Thorn, 2019) Accessed from: https://f.hubspotusercontent00.net/hubfs/7145355/Research/08112020_SG-CSAM_AttitudesExperiences-Report_2019.pdf?__hstc=208625165.851aa734d938b21fee07aa6d05-bc9e7.1604505256798.1614622415296.1614700924025.7&__hssc=208625165.2.1614700924025&__hsfp=723267087 06/05/2021
- 342 A Rapid Assessment of Live Streaming of Online Sexual Abuse and Exploitation of Children and Young People in Kathmandu (ECPAT Luxembourg, ChildSafeNet) Draft, due to be published in 2021. Received by email from ChildSafeNet Nepal, 04/03/2021
- 343 The reception of sexual messages among young Chileans and Uruguayans (Alfaro et al., 2020) Accessed from: https://www.researchgate.net/publication/347336149_The_reception_of_sexual_messages_among_young_Chileans_and_Uruguayans 28/05/2021
- 344 Online Harms White Paper (UK Government, 2019) Accessed from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf 07/05/2021

- 345 Teenage Sexting and Sexual Behaviours in an Iranian Setting (Ghorashi, 2019) Accessed from: https://www.researchgate.net/publication/333826458_Teenage_Sexting_and_Sexual_Behaviors_in_an_Iranian_Setting 19/05/2021
- 346 Demystifying Sexting: Adolescent Sexting and its Associations With Parenting Styles and Sense of Parental Social Control in Israel (Dolev-Cohen and Ricon, 2020) Accessed from: <https://cyberpsychology.eu/article/view/11878/11340> 19/05/2021
- 347 Summary paper on online child sexual exploitation (ECPAT, 2020) Accessed from: <https://www.ecpat.org/wp-content/uploads/2020/12/ECPAT-Summary-paper-on-Online-Child-Sexual-Exploitation-2020.pdf> 22/04/2021
- 348 COVID-19: Child sexual exploitation and abuse threats and trends (Interpol, 2020) Accessed from: <https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-highlights-impact-of-COVID-19-on-child-sexual-abuse> 26/01/2021
- 349 Safe from harm: Tackling webcam child sexual abuse in the Philippines (UNICEF, 2016) Accessed from: <https://www.unicef.org/stories/safe-from-harm-tackling-webcam-child-sexual-abuse-philippines> 09/08/21
- 350 Online sexual abuse of children rising amid COVID 19 pandemic – Save the Children Philippines (Relief Web, 2021) Accessed from: <https://reliefweb.int/report/philippines/online-sexual-abuse-children-rising-amid-covid-19-pandemic-save-children> 22/04/2021
- 351 Technical and Financial Sector Indicators of Livestreaming (IJM, 2020) Shared by IJM, 11/03/2021
- 352 Technical and Financial Sector Indicators of Livestreaming (IJM, 2020) Shared by IJM, 11/03/2021
- 353 Online child sexual abuse and exploitation: Current forms and good practice for prevention and protection (ECPAT, 2017) Accessed from: https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE_ANG-min.pdf 22/04/2021
- 354 Falling short: demand side sentencing for online sexual exploitation of children (International Justice Mission, 2020) Accessed from: <https://www.ijmuk.org/images/EMBAR-GO-8-NOV-20-IJM-REPORT-FALLING-SHORT-Demand-Side-Sentencing-for-Online-Sexual-Exploitation-of-Children.pdf> 15/02/2021
- 355 Online child sexual abuse and exploitation: Current forms and good practice for prevention and protection (ECPAT, 2017) Accessed from: https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE_ANG-min.pdf 22/04/2021
- 356 Victims of livestreamed child sexual abuse (Netclean, 2019) Accessed from <https://www.netclean.com/netclean-report-2019/insight-2/> 22/04/2021
- 357 Summary paper on online child sexual exploitation (ECPAT, 2020) Accessed from: <https://www.ecpat.org/wp-content/uploads/2020/12/ECPAT-Summary-paper-on-Online-Child-Sexual-Exploitation-2020.pdf> 22/04/2021
- 358 UNICEF: What works to prevent online and offline child sexual exploitation and abuse: Review of national education strategies in East Asia and the Pacific (UNICEF, 2020) Accessed from <https://www.sddirect.org.uk/media/1874/what-works-to-prevent-online-and-offline-csae-in-east-asia-and-the-pacific.pdf> 22/04/2021
- 359 UNODC Global Trafficking Report (UNODC, 2021) Accessed from: https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_Chapter5.pdf 22/04/2021
- 360 UNODC Global Trafficking Report (UNODC, 2021) Accessed from: https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_Chapter5.pdf 22/04/2021
- 361 Impact of the COVID 19 pandemic on trafficking in persons (UNODC, 2021) Accessed from: https://www.unodc.org/documents/Advocacy-Section/HTMSS_Thematic_Brief_on_COVID-19.pdf 22/04/2021
- 362 UNODC Global Trafficking Report (UNODC, 2021) Accessed from: https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_Chapter5.pdf 22/04/2021
- 363 Europol Serious and Organised Crime Threat Assessment (SOCTA) 2021 (Europol, 2021) Accessed from: <https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment> 20/04/2021
- 364 National Study of Online Sexual Abuse and Exploitation of Children in the Philippines (UNICEF, 2020) Accessed from: UNICEF Philippines study 22/04/2021
- 365 Why are human trafficking cases difficult to identify and prosecute (John Vanek, 2018) Accessed from: <https://johnvanek.com/2018/01/25/why-are-human-trafficking-cases-difficult-to-identify-and-prosecute/> 11/05/2021
- 366 Summary paper on online child sexual exploitation (ECPAT, 2020) Accessed from: <https://www.ecpat.org/wp-content/uploads/2020/12/ECPAT-Summary-paper-on-Online-Child-Sexual-Exploitation-2020.pdf> 22/04/2021
- 367 Online sexual exploitation of children in the Philippines (IJM, 2020) Accessed from: https://ijmstoragelive.blob.core.windows.net/ijmna/documents/studies/Final-Public-Full-Report-5_20_2020.pdf 22/04/2021
- 368 Cryptocurrency and the Blockchain (International Centre for Missing and Exploited Children, 2017) Accessed from: <https://www.icmec.org/wp-content/uploads/2017/05/IC-MEC-FCACPCryptocurrencyPaperFINAL5-17.pdf> 22/04/2021
- 369 Case Study: The Fintel Alliance – a public private partnership (AUSTRAC, 2021) Shared by the Australian Department of Home Affairs, 19/05/2021
- 370 IJM Composite Case Study - 'Follow the Money' – Trafficking for livestreamed Online Child Sexual Exploitation. Received by email 31/03
- 371 Cryptocurrency and the Blockchain (International Centre for Missing and Exploited Children, 2017) Accessed from: <https://www.icmec.org/wp-content/uploads/2017/05/IC-MEC-FCACPCryptocurrencyPaperFINAL5-17.pdf> 22/04/2021

- 372 Combatting Online Child Sexual Abuse and Exploitation Through Financial Intelligence: Public Bulletin (Egmont Group, 2020) Accessed from: https://egmontgroup.org/sites/default/files/filedepot/20200901_CSAE%20Public%20Bulletin.pdf 16/07/2021
- 373 National Study of Online Sexual Abuse and Exploitation of Children in the Philippines (UNICEF, 2020) Accessed from: UNICEF Philippines study 22/04/2021
- 374 Online child sexual abuse and exploitation: Current forms and good practice for prevention and protection (ECPAT, 2017) Accessed from: https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE_ANG-min.pdf 22/04/2021
- 375 Child Dignity Alliance: Technical Working Group Report (Child Dignity Alliance, 2017) Accessed from: <https://static1.squarespace.com/static/5a4d5d4e7131a5845cd-d690c/t/5c17cdf4032be42f613e28e4/1545063925977/Child+safety+Report+vD+for+web.pdf> 22/04/2021
- 376 Cambodia feared lagging behind predators in cybersex trafficking crackdown (Reuters, 2019) Accessed from: <https://www.reuters.com/article/us-cambodia-sexcrimes-children/cambodia-feared-lagging-behind-predators-in-cybersex-trafficking-crackdown-idUSKCN1VW00B> 22/04/2021
- 377 Informe de monitoreo de país sobre la explotación sexual comercial de niños, niñas y adolescentes (ECPAT, 2014) Accessed from: <https://www.ecpat.org/wp-content/uploads/2016/04/IMP%20MEXICO.pdf> 22/04/2021
- 378 A Global Strategic Response to Online Child Sexual Exploitation and Abuse (WeProtect Global Alliance, 2021) Accessed from: <https://www.weprotect.org/wp-content/uploads/WeProtectGA-Global-Strategic-Response-EN.pdf> 17/06/2021
- 379 Together to #ENDviolence: Global Policy Briefing; Key Messages (The End Violence Partnership, 2020) Received via email from the End Violence Partnership on 13/07/2021
- 380 Guidelines for Medico-Legal Care for Victims of Sexual Violence: Child Sexual Abuse (World Health Organisation, 2003) Accessed from: https://www.who.int/violence_injury_prevention/resources/publications/en/guidelines_chap7.pdf 25/05/2021
- 381 Glossary on Sexual Exploitation and Abuse (United Nations, 2017) Accessed from: https://hr.un.org/sites/hr.un.org/files/SEA%20Glossary%20%20%5BSecond%20Edition%20-%202017%5D%20-%20English_0.pdf 25/05/2021
- 382 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (ECPAT, 2016) Accessed from: https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines_en.pdf 25/05/2021
- 383 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Interagency Working Group on Sexual Exploitation of Children, 2016) Accessed from: https://www.ecpat.org/wp-content/uploads/2016/12/Terminology-guidelines_ENG.pdf (23/07/2021)
- 384 Child Sexual Abuse Material (NCMEC) Accessed from: <https://www.missingkids.org/theissues/csam> 25/05/2021
- 385 IWF Annual Report: Glossary (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/selfgenerated> 06/05/2021
- 386 Non-Photographic Visual Depictions (IWF, 2007) Accessed from: <https://www.iwf.org.uk/what-we-do/who-we-are/consultations/non-photographic-visual-depictions> 25/05/2021
- 387 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (ECPAT, 2016) Accessed from: https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines_en.pdf 25/05/2021
- 388 Grooming (NSPCC) Accessed from: <https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/grooming/> 25/05/2021
- 389 Online Enticement (NCMEC) Accessed from: <https://www.missingkids.org/netsmartz/topics/onlineenticement> 25/05/2021
- 390 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (ECPAT, 2016) Accessed from: https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines_en.pdf 25/05/2021
- 391 What is a deepfake? Everything you need to know about the AI-powered fake media (Business Insider, 2021) Accessed from: <https://www.businessinsider.com/what-is-deepfake?r=US&IR=T#:~:text=Recently%2C%20deepfake%20technology%20has%20been,with%20another%20in%20recorded%20video.> 25/05/2021
- 392 Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic (Europol, 2020) Accessed from: <https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic> 26/01/2021
- 393 Working with Children and Young People Who Have Displayed Harmful Sexual Behaviour (Allardyce and Yates, 2020)
- 394 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (ECPAT, 2016) Accessed from: https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines_en.pdf 25/05/2021
- 395 IWF Annual Report: Glossary (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/selfgenerated> 06/05/2021
- 396 Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children (United Nations, 2000) Accessed from: <https://www.ohchr.org/en/professionalinterest/pages/protocoltraffickinginpersons.aspx>
- 397 Global Threat Assessment 2019 (WePROTECT Global Alliance, 2019) Accessed from: <https://www.weprotect.org/issue/global-threat-assessment/> 25/01/2021

- 398 Global Threat Assessment 2019 (WePROTECT Global Alliance, 2019) Accessed from: <https://www.weprotect.org/issue/global-threat-assessment/> 25/01/2021
- 399 Global Threat Assessment 2019 (WePROTECT Global Alliance, 2019) Accessed from: <https://www.weprotect.org/issue/global-threat-assessment/> 25/01/2021
- 400 Global Threat Assessment 2019 (WePROTECT Global Alliance, 2019) Accessed from: <https://www.weprotect.org/issue/global-threat-assessment/> 25/01/2021
- 401 Global Threat Assessment 2019 (WePROTECT Global Alliance, 2019) Accessed from: <https://www.weprotect.org/issue/global-threat-assessment/> 25/01/2021
- 402 Safer Technology, Safer Users: The UK as a world-leader in Safety Tech (UK Government, 2020) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/887349/Safer_technology__safer_users-The_UK_as_a_world-leader_in_Safety_Tech.pdf 25/05/2021
- 403 Safety by Design (Australian eSafety Commissioner, 2019) Accessed from: <https://www.esafety.gov.au/sites/default/files/2019-10/LOG%207%20-Documents8b.pdf> 25/05/2021
- 404 The Decentralised Web of Hate (Bevensee & Rebellious Data LLC, 2020) Accessed from: <https://rebelliousdata.com/wp-content/uploads/2020/10/P2P-Hate-Report.pdf> 25/05/2021
- 405 What is a VPN? – Virtual Private Network (Cisco) Accessed from: https://www.cisco.com/c/en_uk/products/security/vpn-endpoint-security-clients/what-is-vpn.html 25/05/2021
- 406 Hash Values: Fingerprinting Child Sexual Abuse Material (NetClean, 2018) Accessed from: <https://www.netclean.com/2018/10/30/hash-values/> 25/05/2021
- 407 Hash Values: Fingerprinting Child Sexual Abuse Material (NetClean, 2018) Accessed from: <https://www.netclean.com/2018/10/30/hash-values/> 25/05/2021
- 408 Use of AI in Online Content Moderation (Cambridge Consultants, 2019) Accessed from: https://www.ofcom.org.uk/__data/assets/pdf_file/0028/157249/cambridge-consultants-ai-content-moderation.pdf 25/05/2021
- 409 Darknet Cybercrime Threats to Southeast Asia (UNODC, 2020) Accessed from: https://www.unodc.org/documents/southeastasiaandpacific/Publications/2021/Darknet_Cybercrime_Threats_to_Southeast_Asia_report.pdf 25/05/2021
- 410 End-to-End Encryption (NSPCC, 2021) Accessed from: <https://www.nspcc.org.uk/globalassets/documents/news/e2ee-pac-report-end-to-end-encryption.pdf> 25/05/2021
- 411 IWF Annual Report: Glossary (IWF, 2021) Accessed from: <https://annualreport2020.iwf.org.uk/trends/international/selfgenerated> 06/05/2021
- 412 Metadata (WhatIs.com, 2021) Accessed from: <https://whatis.techtarget.com/definition/metadata> 24/06/2021
- 413 Tor (Investopedia, 2019) Accessed from: <https://www.investopedia.com/terms/t/tor.asp> 07/05/2021
- 414 Convention on the Rights of the Child (United Nations, 1989) Accessed from: <https://www.ohchr.org/en/professionalinterest/pages/crc.aspx> 25/05/2021
- 415 How we protect children's rights with the UN Convention on the Rights of the Child (UNICEF) Accessed from: <https://www.ohchr.org/en/professionalinterest/pages/crc.aspx> 25/05/2021
- 416 Explanatory Notes: General Comment no.25 on children's rights (5Rights Foundation, 2021) Accessed from: https://5rightsfoundation.com/uploads/ExplanatoryNotes_UNCRGC25.pdf 25/05/2021
- 417 Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse (WePROTECT Global Alliance, 2020) Accessed from: <https://www.weprotect.org/response/technology/> 25/05/2021
- 418 Preventing and Tackling Child Sexual Exploitation and Abuse: A Model National Response (WePROTECT Global Alliance, 2016) Accessed from: <https://www.weprotect.org/wp-content/uploads/WePROTECT-Model-National-Response.pdf> 25/05/2021
- 419 Lanzarote Convention (Council of Europe) Accessed from: <https://www.coe.int/en/web/children/lanzarote-convention> 25/05/2021
- 420 Glossary: E-privacy Directive 2009/136/EC (European Data Protection Supervisor) Accessed from: https://edps.europa.eu/data-protection/data-protection/glossary/e_en#e-privacy-directive2009-136-ec 25/05/2021
- 421 The EU will continue to protect children from child sexual abuse online (European Commission, 2020) Accessed from: https://ec.europa.eu/home-affairs/news/20200910_eu-continue-protect-children-from-child-sexual-abuse_en 25/05/2021
- 422 EU Kids Online 2020: Survey Results from 19 Countries (EU Kids Online, 2020) Accessed from: <https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf>
- 423 Production and distribution of child sexual abuse material by parental figures (Australian Institute of Criminology, 2021) Accessed from: https://www.aic.gov.au/sites/default/files/2021-02/ti616_production_and_distribution_of_child_sexual_abuse_material_by_parental_figures.pdf 28/05/2021



***A WeProtect
Global Alliance
reune especialistas
governamentais, do
setor privado e da
sociedade civil.***

***Analizamos problemas
complexos e
desenvolvemos políticas
e soluções para proteger
as crianças contra o
abuso sexual online.***

