

Diretrizes para formuladores de políticas sobre Proteção On-line Infantil 2020



Diretrizes para formuladores de políticas sobre Proteção On-line Infantil

2020

Agradecimentos

Estas diretrizes foram desenvolvidas pela União Internacional de Telecomunicações (UIT) e um grupo de trabalho de autores contribuintes de instituições líderes ativas no setor de tecnologias de informação e comunicação (TIC), bem como em questões de proteção infantil (on-line) e incluiu as seguintes organizações:

ECPAT International, Global Kids On-line network, Global Partnership to End Violence Against Children, project HABLATAM, Insafe network of Safer Internet Centres (Insafe), INTERPOL, the International Centre for Missing & Exploited Children (ICMEC), the International Disability Alliance, a União Internacional de Telecomunicações (UIT), the Internet Watch Foundation (IWF), the London School of Economics, o Escritório do Representante Especial do Secretário-Geral sobre Violência contra Crianças e o Relator Especial sobre a Venda e Exploração Sexual de Crianças, Privately SA, RNW Media, UK Safer Internet Centres, WePROTECT Global Alliance (WPGA) e World Childhood Foundation USA.

O grupo de trabalho foi presidido por David Wright (UK Safer Internet Centres/SWGfL) e coordenado por Fanny Rotino (UIT).

Essas diretrizes não teriam sido possíveis sem o tempo, entusiasmo e dedicação dos autores contribuintes. Contribuições inestimáveis também foram recebidas pelo COFACE-Families Europe, o Conselho da Europa, o Australian eSafety Commissioner, a Comissão Europeia, o e-Worldwide Group (e-WWG), a OCDE, Youth and Media at the Berkman Klein Center for Internet and Society na Universidade de Harvard, bem como governos nacionais individuais e partes interessadas da indústria que compartilham o objetivo comum de tornar a Internet um lugar melhor e mais seguro para crianças e jovens.

A UIT é grata aos seguintes parceiros, que contribuíram com seu valioso tempo e ideias: (listado em ordem alfabética de organização):

- Martin Schmalzried (COFACE-Families Europe)
- Livia Stoica (Conselho da Europa)
- John Carr (ECPAT International)
- Julia Fossi e Ella Serry (Comissárias de Segurança Eletrônica)
- Manuela Marta (Comissão Europeia)
- Salma Abbasi (e-WWG)
- Amy Crocker e Serena Tommasino (Global Partnership to End Violence Against Children)
- Lionel Brossi (HABLATAM)
- Sandra Marchenko (ICMEC)
- Karl Hopwood (Insafe)¹
- Lucy Richardson (International Disability Alliance)

¹ No âmbito do Connecting Europe Facility (CEF), a European Schoolnet gere, em nome da Comissão Europeia, a plataforma Better Internet for Kids, que inclui a coordenação da rede Insafe dos Centros Europeus para uma Internet mais segura (European Safer Internet Centres). Mais informações disponíveis em www.betterinternetforkids.eu

- Matthew Dompier (INTERPOL)
- Fanny Rotino (UIT)
- Tess Leyland (IWF)
- Sonia Livingstone (London School of Economics & Global Kids On-line)
- Elettra Ronchi (OCDE)
- Manus De Barra (Escritório do Representante Especial do Secretário-Geral sobre Violência contra a Criança)
- Deepak Tewari (Privately SA)
- Pavithra Ram (RNW Media)
- Maud De Boer-Buquicchio (Relatora Especial das Nações Unidas sobre a Venda e Exploração Sexual de Crianças)
- David Wright (UK Safer Internet Centres/SWGfL)
- Iain Drennan e Susannah Richmond (WePROTECT Global Alliance)
- Lina Fernandez e Dra. Joanna Rubinstein (World Childhood Foundation, EUA)
- Sandra Cortesi (Youth and Media)

ISBN

978-92-61-30121-7 (versão em papel)

978-92-61-30451-5 (versão eletrônica)

978-92-61-30111-8 (versão EPUB)

978-92-61-30461-4 (versão Mobi)



Por favor leve em consideração o meio ambiente antes de imprimir esse relatório.

© UIT 2020

Alguns direitos reservados. Este trabalho foi licenciado ao público por meio da Creative Commons Attribution-Non-Commercial-Share Alike 3.0 IGO license (CC BY-NC-SA 3.0 IGO).

Sob os termos desta licença, é permitido copiar, distribuir e adaptar o trabalho para fins não comerciais, desde que o trabalho seja devidamente citado, conforme indicado abaixo. Em qualquer utilização deste trabalho, não deve haver nenhuma sugestão de que a UIT apoia qualquer organização, produtos ou serviços específicos. O uso não autorizado de nomes ou logotipos UIT não é permitido. Se você adaptar o trabalho, então você deve licenciar o seu trabalho sob a mesma licença Creative Commons ou equivalente.

“Esta tradução não foi criada pela União Internacional de Telecomunicações (UIT). A UIT não se responsabiliza pelo conteúdo ou a precisão desta tradução. A edição original em inglês será a edição vinculativa e autêntica”.

Para obter mais informações, visite <https://creativecommons.org/licenses/by-nc-sa/3.0/igo/>

Em um mundo onde a Internet permeia quase todos os aspectos da vida moderna, manter os jovens usuários seguros on-line é uma questão cada vez mais urgente para todos os países.

A UIT desenvolveu seu primeiro conjunto de Diretrizes de Proteção Infantil On-line em 2009. Desde aqueles primeiros dias, a Internet evoluiu além de qualquer reconhecimento. Embora tenha se tornado um recurso infinitamente mais rico para as crianças brincarem e aprenderem, também se tornou um lugar muito mais perigoso para elas se aventurarem desacompanhadas.

De questões de privacidade a conteúdo violento e impróprio, a golpistas da Internet e o espectro de aliciamento on-line, abuso e exploração sexual, as crianças de hoje enfrentam muitos riscos. As ameaças estão se multiplicando e os perpetradores operam cada vez mais simultaneamente em muitas jurisdições legais diferentes, limitando a eficácia das respostas e reparações específicas de cada país.

Além disso, a pandemia global da COVID-19 viu um aumento no número de crianças ingressando no mundo on-line pela primeira vez, para auxiliar seus estudos e manter a interação social. As restrições impostas pelo vírus não apenas significaram que muitas crianças mais novas começaram a interagir on-line muito mais cedo do que seus pais poderiam ter planejado, mas a necessidade de conciliar os compromissos de trabalho deixou muitos pais incapazes de supervisionar seus filhos, deixando os jovens em risco de acessar conteúdo impróprio ou ser alvo de criminosos na produção de material de abuso sexual infantil.

Mais do que em qualquer momento anterior, manter as crianças seguras on-line requer uma resposta internacional colaborativa e coordenada, exigindo o envolvimento ativo e o apoio de um amplo número de partes interessadas - desde as partes interessadas da indústria, incluindo plataformas do setor privado, prestadores de serviços e operadores de rede, até governos e a sociedade civil.

Reconhecendo isso, em 2018 os Estados Membros da UIT solicitaram algo mais do que as atualizações oportunas das Diretrizes da POI que foram realizadas periodicamente no passado. Em vez disso, essas novas diretrizes revisadas foram repensadas, reescritas e redesenhadas do zero para refletir as mudanças muito significativas no cenário digital em que as crianças se encontram.

Além de responder aos novos desenvolvimentos em tecnologias e plataformas digitais, esta nova edição aborda uma lacuna importante: a situação enfrentada pelas crianças com deficiência, para as quais o mundo on-line oferece uma salvação particularmente crucial para a plena - e gratificante - participação social. A consideração das necessidades especiais de crianças migrantes e outros grupos vulneráveis também foi incluída.

Para os formuladores de políticas, esperamos que essas diretrizes sirvam como uma base sólida para o desenvolvimento de estratégias nacionais inclusivas e com múltiplas partes interessadas, incluindo consultas abertas e diálogos com crianças, para desenvolver medidas mais bem direcionadas e ações mais eficientes.

Ao desenvolver essas novas diretrizes, a UIT e seus parceiros buscaram criar uma estrutura altamente utilizável, flexível e adaptável, firmemente baseada em padrões internacionais e

metas compartilhadas - particularmente a Convenção sobre os Direitos da Criança e as Metas de Desenvolvimento Sustentável da ONU. No verdadeiro espírito do papel da UIT como uma organizadora global, estou orgulhosa do fato de que essas diretrizes revisadas são o produto de um esforço colaborativo global e são coautoras de especialistas internacionais provenientes de uma ampla comunidade de múltiplas partes interessadas.

Também estou muito feliz em apresentar nosso novo mascote da POI, Sango, um personagem amigável, corajoso e destemido projetado inteiramente por um grupo de crianças, como parte do novo programa internacional de extensão da UIT para jovens.

Em uma época em que mais e mais jovens estão on-line, essas Diretrizes da POI são mais vitais do que nunca. Os formuladores de políticas, a indústria, pais e educadores - e as próprias crianças- todos têm um papel vital a desempenhar. Estou grata, como sempre, por seu apoio e espero continuar nossa estreita colaboração nesta questão crítica.



Doreen Bogdan-Martin
Diretora, Escritório de Desenvolvimento de Telecomunicações

Há trinta anos, quase todos os governos se comprometeram a respeitar, proteger e promover os direitos da criança. A Convenção das Nações Unidas sobre os Direitos da Criança (CDC) é o tratado internacional de direitos humanos mais amplamente ratificado da história. Embora um progresso notável tenha sido alcançado nas últimas três décadas, desafios significativos permanecem e novas áreas de risco para as crianças surgiram.

Em 2015, todas as nações renovaram seu compromisso com as crianças até a agenda de 2030 e as 17 Metas de Desenvolvimento Sustentável (MDS) universais. O Objetivo 16.2, por exemplo, apela para o fim do abuso, exploração e todas as formas de violência e tortura contra crianças até 2030. Mas proteger as crianças é um traço comum em 11 das 17 MDS. O UNICEF coloca as crianças no centro da agenda de 2030, conforme ilustrado na Figura 1.

Figura 1: Crianças, TICs e MDS



A Agenda 2030 para o Desenvolvimento Sustentável reconhece que as TICs podem ser um capacitador-chave para atingir os MDS. A disseminação das tecnologias de informação e comunicação (TICs) e a interconexão global têm o potencial de acelerar o progresso humano, de reduzir a exclusão digital e desenvolver sociedades do conhecimento. Além disso, define metas específicas para o uso de TICs para o desenvolvimento sustentável na educação (Meta 4), igualdade de gênero (Meta 5), infraestrutura (Meta 9 - acesso universal e acessível à Internet) e Meta 17 - parcerias e meios de implementação¹. As TICs têm o poder de transformar profundamente a economia como um todo, sendo uma força motriz na realização de cada uma das 17 MDS. As TICs já deram seu passo ao capacitar bilhões de indivíduos em todo o mundo - fornecendo acesso a recursos de educação e saúde, e serviços como governo eletrônico e mídia social, entre outros.

A explosão da tecnologia da informação e comunicação criou oportunidades sem precedentes para que crianças e jovens se comuniquem, conectem, compartilhem, aprendam, acessem informações e expressem suas opiniões sobre assuntos que afetam suas vidas e suas comunidades.

¹ PNUD, Objetivos de Desenvolvimento Sustentável | UNDP, [undp.org](https://undp.org/content/undp/en/home/sustainable-development-goals.html), accessed January 29, 2020, <https://www.undp.org/content/undp/en/home/sustainable-development-goals.html>; Houlin Zhao, "Why ICTs Are so Crucial to Achieving the SDGs," ITU, ITU News Magazines, 48, accessed January 29, 2020, https://www.itu.int/en/itu-news/Documents/2017/2017-03/2017_ITUNews03-en.pdf

Mas o acesso mais amplo e mais fácil à Internet e à tecnologia móvel também apresenta desafios significativos para a segurança e o bem-estar das crianças - tanto on-line quanto offline.

Para reduzir os riscos do mundo digital e, ao mesmo tempo, permitir que mais crianças e jovens colham seus benefícios, governos, sociedade civil, comunidades locais, organizações internacionais e a indústria devem se unir em um propósito comum. Os formuladores de políticas, em particular, são necessários para atingir uma meta internacional de manter as crianças seguras on-line.

Para responder aos desafios colocados pelo rápido desenvolvimento das TICs e aos desafios da proteção infantil que elas trazem, a iniciativa Proteção On-line Infantil (POI) foi lançada como uma iniciativa internacional com múltiplas partes interessadas pela International Telecommunication Union (UIT) em novembro de 2008. Esta iniciativa visa reunir parceiros de todos os setores da comunidade global para criar uma experiência on-line segura e capacitadora para crianças em todo o mundo.

Além disso, a Conferência de Plenipotenciários da União Internacional de Telecomunicações, realizada em Dubai em 2018, reafirmou a importância da iniciativa da POI, reconhecendo-a como uma plataforma para aumentar a conscientização, compartilhar as melhores práticas e fornecer assistência e apoio aos Estados Membros, especialmente aos países em desenvolvimento, no desenvolvimento e implementação de roteiros da POI. Também reconheceu a importância da proteção de crianças on-line no âmbito da Convenção das Nações Unidas sobre os Direitos da Criança e outros tratados de direitos humanos, incentivando a colaboração entre todas as partes interessadas envolvidas na proteção on-line de crianças.

A Conferência reconheceu a Agenda 2030 para o Desenvolvimento Sustentável, abordando vários aspectos da proteção on-line da criança nas Metas de Desenvolvimento Sustentável (MDS), em particular as MDS 1, 3, 4, 5, 9, 10 e 16; reconheceu ainda a Resolução 175 (Rev. Dubai, 2018), sobre acessibilidade para pessoas com deficiência e pessoas com necessidades específicas de telecomunicações/tecnologia da informação e comunicação (UIT) e a Resolução 67 (Rev. Buenos Aires, 2017) da Conferência Mundial de Desenvolvimento das Telecomunicações (CMDT), sobre o papel do Setor de Desenvolvimento de Telecomunicações da UIT (UIT-D) na proteção on-line de crianças.

No final de 2019, a Comissão de Banda Larga da UIT/UNESCO para o Desenvolvimento Sustentável lançou o Relatório de Segurança Infantil On-line com recomendações viáveis sobre como tornar a Internet mais segura para as crianças.

Em 2009, o primeiro conjunto de diretrizes sobre a proteção on-line de crianças foi emitido pela UIT no contexto da iniciativa POI. Na última década, as Diretrizes da POI foram traduzidas para vários idiomas e utilizadas por muitos países no mundo como um ponto de referência para roteiros e estratégias nacionais relacionadas à proteção on-line de crianças. Eles atenderam a entidades governamentais nacionais, organizações da sociedade civil, instituições de acolhimento de crianças, indústria e muitas outras partes interessadas em seus esforços de proteção on-line de crianças.

Mais especificamente, as diretrizes foram usadas para o esboço, desenvolvimento e implementação de estratégias nacionais de proteção infantil on-line em muitos Estados Membros, como Camarões, Gabão, Gâmbia, Gana, Quênia, Serra Leoa, Uganda e Zâmbia na região da África; Bahrein e Omã na região árabe; Brunei, Camboja, Kiribati, Indonésia,

Malásia, Mianmar e Vanuatu na região Ásia-Pacífico; e Bósnia, Geórgia, Moldávia, Montenegro, Polônia e Ucrânia na região da Europa.

Além disso, as diretrizes construíram a base para eventos regionais, como a Conferência Regional sobre Proteção Infantil On-line (CAPIO): Empoderando os Cidadãos Digitais do Futuro, em Kampala, Uganda (2014), e a Conferência Regional da ASEAN sobre Proteção On-line Infantil realizada em Bangkok, Tailândia (2020).

De acordo com a [Resolução 179](#) (Rev. Dubai, 2018), a UIT em colaboração com os parceiros da iniciativa POI e as partes interessadas foi instruída a atualizar os quatro conjuntos de diretrizes levando em consideração os desenvolvimentos tecnológicos na indústria de telecomunicações, incluindo diretrizes para crianças com deficiência e crianças com necessidades específicas.

Como resultado desse processo, essas diretrizes foram significativamente atualizadas e revisadas por especialistas e partes interessadas relevantes, estabelecendo um amplo conjunto de recomendações para manter as crianças seguras no mundo digital. Eles são o resultado de um esforço colaborativo de várias partes interessadas, aproveitando o conhecimento, a experiência e a especialização de muitas organizações e indivíduos de todo o mundo no campo da proteção on-line de crianças. Eles visam estabelecer as bases para um mundo cibernético seguro e protegido para as gerações futuras. O objetivo deles é atuar como um modelo, que pode ser adaptado e usado de maneira consistente com os costumes e as leis nacionais ou locais. Além disso, essas diretrizes abordam questões que afetam todas as crianças e jovens menores de 18 anos, reconhecendo as diferentes necessidades de cada faixa etária. Além disso, visam atender às necessidades de crianças em diferentes condições de vida e crianças com necessidades especiais e deficiências. As diretrizes também fortalecem o escopo da proteção infantil on-line, abordando todos os riscos, ameaças e danos que as crianças podem encontrar on-line e equilibrando-os cuidadosamente com os benefícios que o mundo digital pode trazer para a vida das crianças.

Espera-se que essas diretrizes não apenas levem à construção de uma sociedade da informação mais inclusiva, mas também possibilitem aos Estados Membros da UIT cumprir suas obrigações de proteger e compreender os direitos das crianças, conforme estabelecido na Convenção das Nações Unidas sobre os Direitos da Criança², adotado pela resolução 44/25 da Assembleia Geral das Nações Unidas de 20 de novembro de 1989 e o [Documento de Resultados da Cúpula Mundial sobre a Sociedade da Informação](#)³ (CMSI).

Ao emitir essas diretrizes, a iniciativa da POI convida todas as partes interessadas a implementar políticas e estratégias que protejam as crianças no espaço cibernético e promovam seu acesso mais seguro a todas as oportunidades extraordinárias que os recursos on-line podem oferecer.

2 UNICEF, "Convention on the Rights of the Child," [unicef.org](https://www.unicef.org/child-rights-convention), accessed January 29, 2020, <https://www.unicef.org/child-rights-convention>.

3 A CMSI foi realizada em duas fases: em Genebra (10-12 de dezembro de 2003) e em Túnis (16-18 de novembro de 2005). A CMSI concluiu com um compromisso ousado "para construir uma sociedade da informação centrada nas pessoas, inclusiva e orientada para o desenvolvimento, onde todos possam criar, acessar, utilizar e compartilhar informações e conhecimento".

Agradecimentos.....	ii
Prefácio	v
Prefácio	vii
Listagem de tabelas, figuras e caixas	xii
1 Visão geral do documento	1
1.1 Objetivo	1
1.2 Âmbito	1
1.3 Princípios gerais	2
1.4 Uso dessas diretrizes	3
2 Introdução	4
2.1 O que é proteção on-line infantil?.....	6
2.2 Crianças no mundo digital	7
2.3 O impacto da tecnologia na experiência digital das crianças	9
2.4 Principais ameaças on-line para crianças.....	10
2.5 Principais danos para crianças on-line.....	13
2.6 Crianças com vulnerabilidades.....	19
2.7 Percepções das crianças sobre os riscos on-line	22
3 Preparando-se para uma estratégia nacional de proteção on-line infantil.....	24
3.1 Atores e partes interessadas	24
3.2 Respostas existentes para proteção on-line infantil	29
3.3 Exemplos de respostas a danos on-line	33
3.4 Benefícios de uma estratégia nacional de proteção on-line infantil.....	33
4 Recomendações para estruturas e implementação	35
4.1 Recomendações de estrutura	35
4.2 Recomendações para implementação.....	38
5 Desenvolvendo uma estratégia nacional de proteção on-line infantil.....	42
5.1 Uma lista de verificação nacional	42
5.2 Exemplos de perguntas.....	50
6 Material de referência.....	51

Listagem de tabelas, figuras e caixas

Tabelas

Tabela 1: Principais áreas a serem consideradas	42
---	----

Figuras

Figura 1: Crianças, TICs e MDS	vi
Figura 2: Classificação de ameaças on-line contra crianças.....	11

Caixas

Acesso à Internet	8
Uso da Internet.....	8
Danos	13

1 Visão geral do documento

1.1 Objetivo

Os governos nacionais têm a obrigação de fornecer proteção às crianças nos mundos físico e virtual. Em um sentido importante, já que as novas tecnologias estão agora completamente integradas às vidas de tantas crianças e jovens de várias maneiras importantes, não faz mais sentido tentar manter distinções rígidas entre eventos do mundo real e eventos on-line. Os dois estão cada vez mais interligados e interdependentes.

Os formuladores de políticas¹ e todas as outras partes interessadas relevantes têm papéis muito importantes a desempenhar. A velocidade com que a tecnologia está evoluindo significa que muitos dos métodos tradicionais de formulação de políticas não servem mais para esse propósito. Os formuladores de políticas devem elaborar uma estrutura legal que seja adaptativa, inclusiva e adequada para a era digital em rápida mudança para proteger as crianças on-line.

O objetivo dessas diretrizes é oferecer aos formuladores de políticas nos Estados membros da UIT uma estrutura flexível e de fácil utilização para compreender e agir de acordo com sua obrigação legal de fornecer proteção às crianças nos mundos real, físico e virtual.

As diretrizes fazem isso abordando várias questões importantes para os formuladores de políticas:

- 1) O que é proteção on-line para crianças?
- 2) Por que eu, como formulador de políticas, preciso me preocupar com a proteção on-line de crianças?
- 3) Qual é o contexto jurídico, sócio-político e de desenvolvimento de meu país?
- 4) Como os formuladores de políticas devem começar a considerar e moldar uma política de proteção on-line eficaz e sustentável para crianças em seu país?

Ao fazer isso, as diretrizes baseiam-se em modelos, estruturas e recursos existentes para oferecer contexto e uma visão a respeito das boas práticas em todo o mundo.

1.2 Âmbito

O âmbito da proteção infantil on-line se estende a qualquer dano a que as crianças sejam expostas on-line, cobrindo uma ampla gama de riscos que ameaçam a segurança e o bem-estar das crianças. É um desafio complexo que deve ser abordado de vários ângulos, incluindo legislação, governança, educação, política e sociedade.

Além disso, a proteção infantil on-line deve ser baseada na compreensão das ameaças, danos e de ambos os riscos gerais e específicos do país que as crianças enfrentam em ambientes digitais. Isso requer definições claras e o estabelecimento de parâmetros claros de intervenção que incluam e diferenciem os atos que constituem um crime e os que, embora não sejam ilegais, representam uma ameaça ao bem-estar da criança.

1 O termo formuladores de políticas refere-se aqui a todas as partes interessadas que são responsáveis pelo desenvolvimento e implementação de políticas, especialmente aqueles dentro do governo.

Para esse fim, as diretrizes fornecem uma visão geral das ameaças e danos atuais que as crianças enfrentam em ambientes digitais. Dito isso, a velocidade com que a tecnologia e as ameaças e danos associados estão evoluindo significa que a velocidade e o método tradicionais de formulação de políticas não conseguem acompanhar o ritmo. Os formuladores de políticas na era digital precisam construir estruturas legais e políticas que sejam adaptáveis e inclusivas o suficiente para enfrentarem os desafios existentes e, tanto quanto possível, antecipar os que virão. Fazer isso requer colaboração com cada uma das partes interessadas, incluindo a indústria de TIC, a comunidade de pesquisa, a sociedade civil, o público e as próprias crianças. Este processo pode ser apoiado pela consideração de princípios abrangentes na proteção on-line de crianças.

1.3 Princípios gerais

Onze princípios transversais estabelecidos aqui, que tomados em conjunto, ajudarão no desenvolvimento de uma estratégia nacional holística de proteção on-line infantil.

A ordem desses princípios reflete uma narrativa lógica em vez de uma ordem de importância. Uma estratégia nacional de proteção on-line infantil deve:

1. basear-se em uma visão holística que incorpore governo, indústria e sociedade;
2. resultar de uma compreensão e análise abrangentes do ambiente digital geral, embora sejam adaptados às circunstâncias e prioridades do país;
3. respeitar e ser consistente com os direitos fundamentais das crianças consagrados na Convenção das Nações Unidas sobre os Direitos da Criança e outras convenções e leis internacionais importantes;
4. respeitar e ser consistente com as leis e estratégias domésticas existentes, semelhantes e relacionadas, como leis de abuso infantil ou estratégias de segurança infantil;
5. respeitar os direitos civis e as liberdades das crianças, que não devem ser sacrificados à proteção;
6. ser desenvolvido com a participação ativa de todas as partes interessadas relevantes, incluindo crianças, abordando suas necessidades e responsabilidades e atendendo às necessidades de grupos minoritários e marginalizados;
7. ser projetado para se alinhar com planos governamentais mais amplos para a prosperidade econômica e social e maximizar a contribuição das TICs para o desenvolvimento sustentável e a inclusão social;
8. utilizar os instrumentos de política disponíveis mais adequados para a realização de seu objetivo, considerando as circunstâncias específicas do país;
9. ser definido no mais alto nível de governo, que será responsável por atribuir funções e responsabilidades relevantes e alocar recursos humanos e financeiros suficientes;
10. ajudar a construir um ambiente digital em que crianças, pais/responsáveis e partes interessadas possam confiar;
11. orientar os esforços das partes interessadas para capacitar e educar as crianças sobre a alfabetização digital para se protegerem on-line.

1.4 Uso dessas diretrizes

Essas diretrizes consideram a pesquisa relevante, os modelos e materiais existentes e estabelecem recomendações claras para o desenvolvimento de uma estratégia nacional de proteção infantil on-line.

- A seção 2 apresenta a proteção infantil on-line e oferece percepções sobre pesquisas recentes, incluindo aspectos relacionados a novas tecnologias emergentes, principais ameaças e danos às crianças.
- A Seção 3 descreve como se preparar para uma estratégia nacional de proteção infantil on-line, incluindo as partes interessadas relevantes, exemplos existentes de respostas a ameaças on-line e danos e benefícios de ter uma estratégia nacional.
- A Seção 4 cobre recomendações para estruturas e implementação.
- A Seção 5 descreve listas de verificação nacionais para desenvolver uma estratégia nacional de proteção infantil on-line.
- A seção 6 fornece materiais de referência úteis.

2 Introdução

Em 2019, mais da metade da população mundial usou a Internet. O maior grupo de usuários é formado por menores de 44 anos, com uso igualmente alto entre os de 16 a 24 anos e de 35 a 44 anos. A nível global, uma em cada três crianças utiliza a Internet (0-18 anos)². Nos países em desenvolvimento, crianças e jovens estão liderando o uso da Internet³ e estima-se que nos próximos cinco anos essa população mais que dobrará. Novas gerações estão crescendo com a Internet e a maioria está se conectando com tecnologia de rede móvel, especialmente no sul global⁴.

Embora o acesso à Internet seja fundamental para a realização dos direitos das crianças, ainda existem significativas disparidades regionais, nacionais, de gênero e outras disparidades de acesso que limitam as oportunidades para meninas, crianças com deficiência, crianças de minorias e outros grupos vulneráveis. Em termos de divisão digital de gênero, a pesquisa mostra que em todas as regiões, exceto nos Estados Unidos da América, os usuários masculinos da Internet superam amplamente os usuários femininos. Em muitos países, as meninas não têm as mesmas oportunidades de acesso que os meninos e, onde têm, as meninas não são apenas monitoradas e restringidas em seu uso da Internet em muito maior grau, mas também podem ter sua segurança em risco nas tentativas de acesso à Internet⁵. É claro que crianças e jovens sem habilidades digitais ou que falam línguas minoritárias não podem encontrar facilmente conteúdo relevante on-line e que crianças de áreas rurais possuem menos habilidades digitais, passam mais tempo on-line (especialmente jogando) e recebem menos mediação e monitoramento⁶ dos pais.

No entanto, nenhuma conversa sobre riscos e ameaças pode ocorrer sem reconhecer a natureza tremendamente enriquecedora e fortalecedora da tecnologia digital. A Internet e as tecnologias digitais estão transformando a maneira como vivemos e tornaram acessível muitas novas maneiras de se comunicar, jogar, curtir música e se envolver em uma vasta gama de atividades culturais, educacionais e de aprimoramento de habilidades. A Internet pode fornecer acesso crucial a serviços de saúde e educacionais, assim como informações sobre tópicos que são importantes para os jovens, mas podem ser tabu em suas sociedades.

2 OCDE, "New Technologies and 21st Century Children: Recent Trends and Outcomes," OECD Education Working Paper No. 179 (Directorate for Education and Skills, OECD), accessed January 27, 2020, <https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=EDU/WKP%282018%2915&docLanguage=En>.

3 Ofcom, "Children and Parents: Media Use and Attitudes Report 2018" (Ofcom), accessed January 17, 2020, https://www.ofcom.org.uk/__data/assets/pdf_file/0024/134907/children-and-parent-media-use-and-attitudes-2018.pdf.

4 UIT, "Measuring the Information Society Report," accessed January 16, 2020 https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICTOI-2018-SUM-PDF-E.pdf.

5 "Young Adolescents and Digital Media: Uses, Risks and Opportunities in Low-and Middle-Income countries," GAGE, accessed January 29, 2020, <https://www.gage.odi.org/publication/digital-media-risks-opportunities/>.

6 Livingstone, S., Kardefelt Winther, D. e Hussein, M. (2019). Global Kids On-line Comparative Report, Innocenti Research Report. UNICEF Office of Research - Innocenti, Florence, <https://www.unicef-irc.org/publicações/1059-global-kids-on-line-comparative-report.html>. Isso pode ter resultados inesperados, por exemplo, uma pesquisa realizada pela HABLATAM em cinco países latino-americanos mostrou que, em comunidades vulneráveis, as crianças podem estar usando plataformas de namoro, videogames e redes sociais para realizar transações de dinheiro para fins ilegais. Rede Contactados al Sur, "Hablatam," Hablatam Project 2020, accessed February 6, 2020, <https://hablatam.net/>.

Assim como crianças e jovens muitas vezes estão na vanguarda da adoção e adaptação às novas possibilidades oferecidas pela Internet, eles também estão sendo expostos a uma série de questões relacionadas à segurança e ao bem-estar que devem ser reconhecidas e enfrentadas pela sociedade. É essencial discutir abertamente os riscos que existem para crianças e jovens on-line. A discussão abre uma plataforma a partir da qual crianças e jovens podem ser ensinados a reconhecer o risco e prevenir ou lidar com os danos caso eles se materializem, bem como as vantagens e oportunidades que a Internet pode oferecer.

Em muitas partes do mundo, os jovens têm uma boa compreensão de alguns dos riscos que enfrentam on-line.^{7,8} A pesquisa mostrou, por exemplo, que a maioria das crianças e jovens são capazes de distinguir o cyberbullying das piadas ou provocações on-line. Eles reconhecem que o cyberbullying tem uma dimensão pública e é projetado para causar danos, mas equilibrar as oportunidades e os riscos on-line de uma criança continua a ser um desafio⁹.

Para os Estados-Membros da UIT, a proteção de crianças e jovens on-line continua a ser uma prioridade, que deve ser cuidadosamente equilibrada com os esforços para promover oportunidades para crianças e jovens on-line¹⁰, e deve ser feita de uma forma que proteja crianças e jovens sem afetar seu acesso ou o acesso do público em geral à informação, ou a capacidade de desfrutar da liberdade de expressão e associação.

Há uma necessidade óbvia de investimento dedicado e soluções criativas para lidar com os riscos enfrentados por crianças e jovens, principalmente por causa da divisão digital entre crianças e adultos que limita a orientação de pais, professores e responsáveis. Ao mesmo tempo, à medida que crianças e jovens crescem e se tornam adultos, pais e membros ativos da sociedade, existe uma oportunidade potencial e imperdível para eles reduzirem a exclusão digital.

Diante disso, o desenvolvimento da confiança na Internet deve estar na vanguarda e no centro das políticas públicas. Os governos e a sociedade precisam trabalhar com as crianças e os jovens para compreender suas perspectivas e estimular um debate público genuíno sobre riscos e oportunidades. Apoiar crianças e jovens na gestão de riscos on-line pode ser eficaz, mas os governos devem também garantir que haja serviços de apoio adequados para aqueles que sofrem danos on-line e que as crianças saibam como acessar esses serviços.

Alguns países têm dificuldade para alocar recursos suficientes para lidar com a alfabetização digital e a segurança das crianças on-line. No entanto, as crianças relatam que pais, professores, empresas de tecnologia e governos são atores importantes no desenvolvimento de soluções para apoiar sua segurança on-line. Os Estados-Membros da UIT indicaram também que existe um apoio significativo para uma maior partilha de conhecimentos e esforços coordenados para garantir a segurança de um maior número de crianças on-line.

Crianças e jovens estão navegando em um cenário digital cada vez mais complexo e a adoção de inteligência artificial para aprendizado de máquina, análise de big data, robótica, realidade

7 Desde 2016, a UIT realiza consultas dentro da POI com crianças e adultos interessados sobre questões relevantes, como cyberbullying, alfabetização digital e atividades infantis on-line.

8 ITU, Youth Consultation, <https://www.itu.int/en/council/cwg-cop/Pages/meetings.aspx>.

9 UNICEF, "Global Kids On-line Comparative Report (2019)."

10 UIT, "Celebrating 10 Years of Child On-line Protection", ITU News, 6 de fevereiro de 2018, <https://news.itu.int/celebration-10-year-child-on-line-protection/>.

virtual e aumentada e a Internet das Coisas estão prontas para transformar as práticas de mídia infantil. Isso requer formulação de políticas e investimentos para as crianças, pais e comunidades do futuro, tanto quanto hoje.

2.1 O que é proteção on-line infantil?

As tecnologias on-line apresentam muitas possibilidades para crianças e jovens se comunicarem, aprenderem novas habilidades, ser criativos e contribuir para uma sociedade melhor. Mas também podem trazer novos riscos, como expô-los a questões de privacidade, conteúdo ilegal, assédio, cyberbullying, uso indevido de dados pessoais ou aliciamento para fins sexuais e até mesmo abuso sexual infantil.

Essas diretrizes desenvolvem uma abordagem holística para responder a todas as ameaças e danos potenciais que crianças e jovens podem encontrar ao adquirir a alfabetização digital. Elas reconhecem que todas as partes interessadas relevantes têm um papel em sua resiliência digital, bem-estar e proteção, enquanto se beneficiam das oportunidades que a Internet pode oferecer.

Proteger as crianças e os jovens é uma responsabilidade compartilhada e cabe a todas as partes interessadas relevantes garantir um futuro sustentável para todos. Para que isso aconteça, os formuladores de políticas, a indústria, pais, responsáveis, educadores e outras partes interessadas devem garantir que as crianças e os jovens possam alcançar seu potencial - on-line e offline.

Embora não exista uma definição universal para a proteção on-line de crianças, o objetivo é uma abordagem holística para a construção de espaços digitais seguros, adequados à idade, inclusivos e participativos para crianças e jovens, caracterizados por:

- resposta, apoio e autoajuda diante de ameaças;
- prevenção de danos;
- um equilíbrio dinâmico entre garantir proteção e oferecer oportunidades para as crianças serem cidadãos digitais;
- defender os direitos e as responsabilidades das crianças e da sociedade.

Além disso, devido aos rápidos avanços na tecnologia e na sociedade e à natureza sem fronteiras da Internet, a proteção on-line infantil precisa ser ágil e adaptável para ser eficaz. Embora essas diretrizes ofereçam compreensão sobre os principais riscos para crianças e jovens on-line, incluindo conteúdo prejudicial e ilegal, assédio, cyberbullying, uso indevido de dados pessoais ou aliciamento para fins sexuais e abuso e exploração sexual infantil, novos desafios surgirão com o desenvolvimento de inovações tecnológicas e normalmente variam de região para região. No entanto, a melhor maneira de lidar com novos desafios é trabalhar em conjunto como uma comunidade global, pois novas soluções para esses desafios precisam ser encontradas.

2.2 Crianças no mundo digital

A Internet transformou a forma como vivemos. Está totalmente integrada na vida de crianças e jovens, tornando impossível considerar os mundos digital e físico separadamente. Um terço de todos os usuários da Internet hoje são crianças e jovens, e o UNICEF estima que 71 por cento dos jovens já estão on-line.

Tal conectividade tem sido extremamente empoderadora. O mundo on-line permite que crianças e jovens superem desvantagens e deficiências, e tem oferecido novas áreas para entretenimento, educação, participação e construção de relacionamento. As plataformas digitais, hoje, são usadas para uma variedade de atividades e muitas vezes são experiências multimídia.

Ter acesso e aprender a usar e navegar por essa tecnologia é considerado crítico para o desenvolvimento dos jovens e tais plataformas são usadas pela primeira vez na infância. Os formuladores de políticas devem compreender que crianças e jovens geralmente começam a usar plataformas e serviços antes de atingirem a idade mínima definida e, portanto, a educação deve começar cedo.

Crianças e jovens querem estar envolvidas na conversa e têm conhecimentos valiosos como 'nativos digitais' que podem ser compartilhados. Os formuladores de políticas e profissionais devem se envolver com crianças e jovens em um debate contínuo sobre o ambiente on-line para apoiar seus direitos.

Acesso à Internet

Em 2019, mais da metade da população mundial usou a Internet (53,6 por cento), com uma estimativa de 4,1 bilhões de usuários. Em nível global, um em cada três usuários da Internet é uma criança menor de 18 anos¹. Em alguns países de renda mais baixa, isso aumenta para cerca de um em dois, enquanto nos países de renda mais alta, a proporção é de cerca de um em cinco. De acordo com o UNICEF, mundialmente, 71 por cento dos jovens já estão on-line². As crianças e os jovens são, portanto, agora uma presença substancial, permanente e constante na Internet³. A Internet serve a outros fins sociais, econômicos ou políticos e tornou-se uma família ou produto de consumo ou serviço que é essencial para o jeito como famílias, crianças e jovens vivem suas vidas.

Em 2017, regionalmente, o acesso de crianças e jovens à Internet está altamente vinculado ao nível de renda. Os países de baixa renda tendem a ter menos usuários infantis da Internet do que os países de alta renda.

Crianças e jovens na maioria dos países passam mais tempo on-line no fim de semana do que em um dia de semana, com adolescentes (15-17 anos) passando mais tempo on-line, entre 2,5 e 5,3 horas em média, dependendo do país.

Uso da Internet

Entre crianças e jovens, o dispositivo de acesso à Internet mais popular é o celular, seguido por computadores desktop e laptops. Crianças e jovens passam, em média, cerca de duas horas por dia on-line durante a semana e quase o dobro em cada dia do fim de semana. Alguns se sentem permanentemente conectados. Mas muitos outros ainda não têm acesso à Internet em casa.

Na prática, a maioria das crianças e jovens que usam a Internet acessam-na por meio de mais de um dispositivo: Crianças e jovens que se conectam pelo menos uma vez por semana, às vezes usam até três dispositivos diferentes para fazer isso. Crianças mais velhas e crianças em países mais ricos geralmente usam mais dispositivos, e os meninos usam um pouco mais dispositivos do que as meninas em todos os países pesquisados.

- 1 Livingstone, S., Carr, J., and Byrne, J. (2015) One in three: The task for global internet governance in addressing children's rights. Global Commission on Internet Governance: Paper Series. London: CIGI and Chatham House, <https://www.cigion-line.org/publications/one-three-internet-governance-and-childrens-rights>.
- 2 Broadband Commission, "Child On-line Safety: Minimizing the Risk of Violence, Abuse and Exploitation On-line (2019)," Broadband Commission for Sustainable Development, October 2019, 84, https://broadbandcommission.org/Documents/working-groups/ChildOn-lineSafety_Report.pdf.
- 3 Livingstone, Carr and Byrne, "One in Three: Internet Governance and Children's Rights."

A atividade mais popular - para meninas e meninos - é assistir a vídeos. Mais de três quartos das crianças e jovens que usam a Internet dizem que assistem a vídeos on-line pelo menos uma vez por semana, sozinhos ou com outros membros da família. Muitas crianças e jovens podem ser considerados 'socializadores ativos' usando várias plataformas de mídia social, como Facebook, Twitter, TikTok ou Instagram.

Crianças e jovens também se envolvem na política on-line e fazem suas vozes serem ouvidas por meio de blogs.

O nível geral de participação em jogos on-line varia de acordo com o país, de acordo com a disponibilidade de acesso à Internet por crianças e jovens, enquanto 10 a 30 por cento das crianças e jovens usuários da Internet se envolvem em atividades on-line criativas semanalmente.

Para fins educativos, muitas crianças e jovens de todas as idades usam a Internet para fazer a lição de casa, ou mesmo para recuperar o atraso após faltar às aulas ou buscar informações de saúde on-line semanalmente. As crianças mais velhas parecem ter maior apetite por informações do que as crianças mais novas.

2.3 O impacto da tecnologia na experiência digital das crianças

A Internet e a tecnologia digital podem oferecer oportunidades e apresentar riscos para crianças e jovens. Por exemplo, quando as crianças usam as mídias sociais, elas se beneficiam de muitas oportunidades para explorar, aprender, comunicar e desenvolver habilidades importantes. Por exemplo, as redes sociais são vistas pelas crianças como plataformas que lhes permitem explorar a identidade pessoal em um ambiente seguro. Ter as competências relevantes e saber como lidar com questões relacionadas com privacidade e reputação é importante para os jovens.

"Sei que tudo que você posta na Internet fica para sempre e pode afetar sua vida no futuro",
Menino, 14 anos, Chile.

No entanto, com consultas que mostram que a maioria das crianças usa as redes sociais antes dos treze anos de idade¹¹, e os serviços de verificação de idade são geralmente fracos ou inexistentes, os riscos que as crianças enfrentam podem ser intensificados. E embora as crianças queiram aprender habilidades digitais e se tornarem cidadãos digitais, em particular se preocupando com sua privacidade, elas tendem a pensar sobre privacidade em relação a seus amigos e conhecidos - "O que meus amigos podem ver?" - e menos ainda em relação a estranhos e terceiros. Combinado com a curiosidade natural das crianças e geralmente mais baixo limiar de risco, isso pode torná-las vulneráveis a aliciamento, exploração, bullying ou outros tipos de conteúdo ou contato prejudicial.

A ampla popularidade do compartilhamento de imagens e vídeos por meio de aplicativos móveis e, particularmente, o uso de plataformas de transmissão ao vivo por crianças apresenta mais preocupações relacionadas a riscos e privacidades. Algumas crianças estão produzindo imagens sexuais de si mesmas, de amigos e irmãos e as compartilham on-line. Para alguns, principalmente crianças mais velhas, isso pode ser visto como a exploração natural da

11 Rede Conectados al Sur, "Hablatam"; UNICEF, "Global Kids On-line Comparative Report (2019)."

sexualidade e da identidade sexual, enquanto para outros, especialmente as crianças mais novas, muitas vezes há coerção por um adulto ou outra criança. Seja qual for o caso, o conteúdo resultante é ilegal em muitos países e pode expor as crianças ao risco de processo judicial ou pode ser usado para explorar ainda mais a criança.

Da mesma forma, os jogos on-line permitem que as crianças cumpram o seu direito fundamental de jogar, bem como de construir redes, de passar tempo e conhecer novos amigos e desenvolver habilidades importantes. Incrivelmente, isso pode ser positivo. No entanto, há cada vez mais evidências que indicam que, se deixadas sem monitoramento e sem o apoio de um adulto responsável, as plataformas de jogos on-line também podem representar riscos para as crianças, desde transtornos de jogos, riscos financeiros, coleta e monetização de dados pessoais de crianças, até cyberbullying, discurso de ódio, violência e exposição a conduta ou conteúdo impróprio¹², e aliciamento usando imagens e vídeos reais, gerados por computadores ou mesmo de realidade virtual, que retratam e normalizam o abuso e a exploração sexual de crianças.

Além disso, os desenvolvimentos na tecnologia levaram ao surgimento da Internet das Coisas, onde um número e uma variedade cada vez maiores de dispositivos são capazes de se conectar, comunicar e criar redes pela Internet. Isso inclui brinquedos, monitores para bebês e dispositivos alimentados por inteligência artificial que podem apresentar riscos em termos de privacidade e contato indesejado.

2.4 Principais ameaças on-line para crianças

Adultos e crianças estão expostos a uma série de riscos e perigos on-line. No entanto, as crianças são uma população muito mais vulnerável. Algumas crianças também são mais vulneráveis do que outros grupos de crianças, por exemplo, crianças com deficiência¹³ ou crianças deslocadas. Os formuladores de políticas precisam garantir que todas as crianças possam se desenvolver e serem educadas em um ambiente digital seguro. A ideia de que as crianças são vulneráveis e devem ser protegidas de todas as formas de exploração está delineada na Convenção das Nações Unidas sobre os Direitos da Criança.

Várias áreas do ambiente digital oferecem grandes oportunidades para as crianças, mas podem, ao mesmo tempo, aumentar os riscos que podem prejudicar profundamente as crianças e comprometer seu bem-estar. Há preocupações, tanto para adultos como para crianças, de que, por exemplo, a Internet possa ser usada para invadir a privacidade pessoal, espalhar desinformação ou, pior, permitir o acesso à pornografia.

É fundamental aqui distinguir entre riscos e danos para as crianças. Nem todas as atividades que podem conter elementos de risco são perigosas e nem todos os riscos se tornam necessariamente prejudiciais para as crianças, por exemplo, Sexting, que é uma forma que os jovens podem explorar a sexualidade e os relacionamentos, e que não é necessariamente prejudicial.

12 UNICEF, "Global Kids On-line Comparative Report (2019)." (UNICEF, 2019)

13 Lundy et al., "TWO CLICKS FORWARD AND ONE CLICK BACK," Report on children with disabilities in the digital environment (Council of Europe, October 2019), <https://rm.coe.int/two-clicks-forward-and-one-click-back-report-on-children-with-disabili/168098bd0f>.

Figura 2: Classificação de ameaças on-line contra crianças¹⁴

	Conteúdo <i>Criança como recipiente (de produções em massa)</i>	Contato <i>Criança como participante (atividade iniciada por adulto)</i>	Conduta <i>Criança como ator (autor/vítima)</i>
Agressivo	Conteúdo violento/sangrento	Assédio, perseguição	Bullying, atividade hostis de amigos e conhecidos
Sexual	Conteúdo pornográfico	Aliciamento, abuso sexual ao encontrar estranhos	Assédio sexual, "sexting"
Valores	Conteúdo racista/de ódio	Persuasão ideológica	Conteúdo gerado pelo usuário potencialmente danoso
Comercial	Propaganda, marketing embutido	Exploração e mau uso de dados pessoais	Jogos de azar, violação de direitos autorais

Fonte: EU Kids On-line (Livingstone, Haddon, Görzig and Ólafsson [2011])

O advento da era digital apresentou novos desafios para a proteção da criança. As crianças devem ser empoderadas para navegar no mundo on-line com segurança e colher suas muitas recompensas.

Os formuladores de políticas devem garantir que a legislação, salvaguardas e ferramentas relevantes estejam em vigor para permitir que as crianças se desenvolvam e aprendam com segurança. É fundamental que as crianças sejam equipadas com as habilidades necessárias para identificar ameaças e compreender totalmente as implicações e nuances de seu comportamento on-line.

Enquanto estão on-line, as crianças podem encontrar uma infinidade de ameaças vindas de organizações, adultos e de seus colegas.

Conteúdo e manipulação

- A exposição a conteúdo impróprio ou mesmo criminoso pode levar as crianças a extremos, como automutilação, comportamentos destrutivos e violentos. A exposição a esse tipo de conteúdo pode igualmente levar à radicalização ou adesão a ideias racistas ou discriminatórias. É reconhecido que muitas crianças não respeitam as limitações de idade colocadas nos sites.
- A exposição a informações imprecisas ou incompletas limita a compreensão das crianças sobre o mundo ao seu redor. A tendência de personalizar o conteúdo com base no comportamento do usuário pode levar a 'bolhas de filtro', restringindo as crianças de desenvolver e acessar uma ampla gama de conteúdo.
- A exposição ao conteúdo filtrado por algoritmos com a intenção de manipular pode influenciar muito o desenvolvimento, as opiniões, os valores e os hábitos de uma criança. Isolar crianças em 'câmaras de eco' ou 'bolhas de filtro' impede que tenham acesso a uma ampla variedade de opiniões e ideias.

¹⁴ Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011). Risks and safety on the internet: The perspective of European children. Full findings. LSE, London: EU Kids On-line, <http://eprints.lse.ac.uk/33731/>.

Contato de adultos ou colegas

As crianças podem encontrar uma ampla gama de ameaças de contato vindas de seus colegas ou adultos.

- O bullying on-line pode se espalhar mais amplamente, com um grau maior de velocidade, do que offline. Pode acontecer a qualquer hora do dia ou da noite, invadindo assim espaços anteriormente 'seguros', e pode ser anônimo.
- Crianças que são vítimas offline provavelmente serão vítimas on-line. Isso coloca as crianças com deficiência em maior risco on-line, já que pesquisas mostram que crianças com deficiência estão mais propensas a sofrer abuso de qualquer tipo e, especificamente, estão mais propensas a sofrer vitimização sexual. A vitimização pode incluir intimidação, assédio, exclusão e discriminação com base na deficiência real ou percebida de uma criança, ou em aspectos relacionados à deficiência, como a maneira como se comportam ou falam, ou os equipamentos ou serviços que usam.
- Difamação e danos à reputação: imagens e vídeos podem ser alterados e compartilhados com bilhões de pessoas. Comentários mal feitos podem ficar disponíveis por décadas, gratuitamente para qualquer pessoa ver.
- As crianças podem ser visadas, tratadas e abusadas pela Internet por um criminoso local ou do outro lado do mundo, muitas vezes alegando ser alguém que não é. Isso pode assumir várias formas, incluindo radicalização ou ser coagida a enviar conteúdo sexualmente explícito de si mesmo.
- Ser pressionada, enganada ou coagida a fazer compras com ou sem a permissão do pagador.
- A publicidade indesejada levanta questões de consentimento e venda de dados.

Conduta da criança, potencialmente levando a consequências

- O bullying on-line pode ser particularmente perturbador e prejudicial porque pode se espalhar mais amplamente, com um maior grau de publicidade, e o conteúdo circulado eletronicamente pode ressurgir a qualquer momento, o que pode tornar mais difícil para a vítima do bullying conseguir superar o incidente; pode conter imagens visuais prejudiciais ou palavras ofensivas; o conteúdo está disponível 24 horas por dia; o bullying por meios eletrônicos pode acontecer 24 horas por dia, 7 dias por semana, de forma que pode invadir a privacidade da vítima, mesmo em locais "seguros" como sua casa; e informações pessoais podem ser manipuladas, imagens visuais alteradas e, então, repassadas a outras pessoas. Além disso, pode ser realizado de forma anônima. Divulgação de informações pessoais que levem ao risco de danos físicos, incluindo encontros na vida real com conhecidos on-line, com a possibilidade de abuso físico e/ou sexual.
- Violação dos próprios direitos ou de terceiros por meio de plágio e envio de conteúdo sem permissão, incluindo a captura e envio de fotos inadequadas sem permissão.
- Violação dos direitos autorais de outras pessoas, por exemplo, ao baixar músicas, filmes ou programas de TV que deveriam ser pagos, pois isso pode ser prejudicial para a vítima do roubo.

- Uso compulsivo e excessivo da Internet e/ou jogos on-line, em detrimento de atividades sociais e/ou ao ar livre importantes para a saúde, construção de confiança, desenvolvimento social e bem-estar geral.
- Tentar ferir, assediar ou intimidar outra pessoa, incluindo fingir ser outra pessoa, geralmente outra criança.
- Um comportamento cada vez mais comum entre os adolescentes é o 'sexting' (compartilhamento de imagens ou textos sexualizados por meio de telefones celulares). Essas imagens e textos são frequentemente compartilhados entre parceiros em um relacionamento ou com parceiros em potencial, mas às vezes acabam sendo compartilhados com públicos muito mais amplos. É improvável que os adolescentes tenham uma compreensão adequada das implicações desses comportamentos e dos riscos potenciais que eles acarretam.

2.5 Principais danos para crianças on-line

A seção anterior se refere às ameaças que as crianças podem encontrar on-line. Esta seção destaca os danos que podem ocorrer dessas ameaças.

Danos

De acordo com estudos do UNICEF sobre o uso da Internet, as seguintes categorias são consideradas riscos e danos:

- Auto-abuso e automutilação:

- conteúdo suicida
- discriminação

- Exposição a materiais inadequados:

- exposição a conteúdo extremista/violento/sangrento
- marketing embutido
- jogos de azar on-line

- Cerca de 20 por cento das crianças pesquisadas sobre o assunto disseram ter visto, no ano passado, sites ou discussões on-line sobre pessoas que se machucaram ou causaram danos a si mesmo fisicamente.

- Radicalização:

- persuasão ideológica
- discurso de ódio

- As crianças eram mais propensas a relatar que ficaram chateadas com discurso de ódio ou conteúdo sexual

on-line, sendo tratadas de forma prejudicial on-line ou offline ou encontrando-se pessoalmente com alguém que conheceram on-line.

abuso sexual e exploração:

- conteúdo auto-gerado

- Aliciamento sexual
- material de abuso sexual infantil (MASI)
- tráfico
- exploração sexual de crianças em viagens e turismo

Um estudo de 2017 com crianças na Dinamarca, Hungria e Reino Unido descobriu que 6% das crianças tiveram fotos explícitas delas compartilhadas sem sua permissão.

Em 2019, a Internet Watch Foundation (IWF) identificou mais de 132.000 páginas da web confirmadas como contendo imagens e vídeos de abuso sexual infantil. Cada página da web pode conter de uma a milhares de imagens desse abuso.

Os riscos relacionados à violência on-line, como a divulgação de fotos nuas sem consentimento e cyber-bullying sexual, são marcados por dinâmicas de gênero desiguais, com as meninas geralmente sendo mais afetadas por pressões de gênero em relação ao comportamento sexual, experimentando consequências que são mais negativas e causadoras de prejuízo.

- Violação e uso indevido de dados pessoais:

- hacking
- fraude e roubo

Muitas pessoas estão familiarizadas com golpes e hackers, mas a invasão de privacidade relacionada às atividades on-line de uma criança é vista como outra violação. Os adultos muitas vezes prejudicam os jovens examinando seus telefones celulares e pesquisando suas atividades on-line. Por exemplo, relatórios de crianças no Brasil mostram que meninos e meninas, de diferentes faixas etárias, percebem os pais como mais controladores quando meninas usam a Internet. As tentativas de explicar isso geralmente sugerem que as meninas podem ser, em alguns casos, mais vulneráveis devido às estruturas sociais nas quais vivem, em particular no que diz respeito à sua segurança, em um contexto onde a fronteira entre a interação on-line e offline torna-se cada vez mais tênue.

- Cyberbullying, perseguição e assédio: atividade hostil e violenta de colegas

As salas de bate-papo e os sites de redes sociais podem abrir as portas para a violência e o bullying, já que usuários anônimos, incluindo jovens, se envolvem em comunicação agressiva ou abusiva. Em sete países da Europa - Bélgica, Dinamarca, Irlanda, Itália, Portugal, Romênia e Reino Unido - Livingstone, Mascheroni, Ólafsson e Haddon¹ descobriram que, em média, em 2010, 8 por cento das crianças foram vítimas de cyberbullying, enquanto 12 por cento das crianças foram vítimas de cyberbullying em 2014.

É essencial destacar que as crianças vulneráveis muitas vezes correm um risco maior de vitimização por cyberbullying.

1 Livingstone, S., Mascheroni, G., Ólafsson, K., and Haddon, L., (2014) Children's on-line risks and opportunities: comparative findings from EU Kids On-line and Net Children Go Mobile. London: London School of Economics and Political Science, www.eukidson-line.net and hYp://www.netchildrengomobile.eu/.

Em foco: Realçando as desigualdades

Em 2017, cerca de 60 por cento das crianças não estavam on-line na região da África, em comparação com apenas 4 por cento na Europa. Os usuários masculinos da Internet superaram os usuários femininos em todas as regiões do mundo, e o uso da Internet por meninas é frequentemente monitorado e restrito. Com a expansão da banda larga para as partes não conectadas do mundo, essa desigualdade aumentará significativamente ¹⁵.

As crianças que dependem de telefones celulares em vez de computadores podem ter uma experiência on-line de segunda melhor qualidade. Crianças que falam línguas minoritárias geralmente não conseguem encontrar conteúdo relevante on-line, e crianças de áreas rurais são mais propensas a vivenciar roubo de senhas ou dinheiro.

A pesquisa mostra que muitos adolescentes em todo o mundo devem superar barreiras significativas para sua participação on-line. Para muitos, os desafios de acesso - conectividade ruim, custos excessivos de dados e dispositivos e falta de equipamento apropriado - continuam sendo barreiras importantes.

Com a expansão da banda larga acessível para o mundo em desenvolvimento, há uma necessidade urgente de implementar medidas para minimizar os riscos e ameaças a essas crianças, ao mesmo tempo lhes permitindo capitalizar todos os benefícios do mundo digital.

Em foco: Material de Abuso Sexual Infantil (MASI)

A dimensão do problema

A Internet transformou a escala e a natureza da produção, distribuição e disponibilidade de MASI. Em 2018, empresas de tecnologia com sede nos Estados Unidos da América relataram mais de 45 milhões de imagens e vídeos on-line suspeitos de mostrar crianças sendo abusadas sexualmente em todo o mundo. Esta é uma indústria global e a proporção e a gravidade do abuso estão aumentando, apesar dos esforços para impedi-lo.

Historicamente, em um mundo offline, encontrar MASI exigia que os infratores assumissem riscos consideráveis, com custos significativos, para acessar o material. Com a Internet, os infratores agora podem acessar esse material com relativa facilidade e se envolver em comportamentos cada vez mais arriscados. As câmeras são menores, cada vez mais integradas a todos os aspectos de nossas vidas, tornando o processo de produção de MASI e aquisição de conteúdo de abuso sem contato mais fácil do que nunca.

É impossível determinar o tamanho ou a forma precisa dessa empresa clandestina e ilegal. No entanto, é claro que o número de imagens ilegais agora em circulação pode ser contado na casa dos milhões. Quase todas as crianças envolvidas nas imagens tiveram suas imagens duplicadas. Em 2018, o IWF rastreou a frequência com que surgiam imagens de uma criança conhecida por ter sido resgatada em 2013. Ao longo dos três meses, os analistas do IWF rastrearam as imagens 347 vezes - 5 vezes todos os dias úteis.

15 Broadband Commission, "Child On-line Safety: Minimizing the Risk of Violence, Abuse and Exploitation On-line (2019)."

O cenário atual

Cada vez que a imagem de uma criança sendo abusada aparece e reaparece on-line, ou é baixada por um criminoso, essa criança está sendo abusada novamente. As vítimas são obrigadas a conviver com a longevidade e a circulação dessas imagens pelo resto de suas vidas.

Assim que for descoberto um material que retrate ou uma página da web que hospeda o abuso sexual infantil, é importante remover ou bloquear o conteúdo o mais rápido possível. A natureza global da Internet torna isso difícil: os infratores podem produzir material em um país e hospedá-lo em outro para consumidores em um terceiro. É quase impossível que autorizações ou notificações nacionais sejam promulgadas sem uma cooperação internacional sofisticada.

O ritmo da inovação no mundo digital significa que o cenário do infrator está em constante mudança. As principais ameaças que surgiram recentemente incluem:

- O aumento da criptografia permite inadvertidamente que os infratores operem e compartilhem material com canais ocultos, enquanto torna a detecção e a aplicação da lei mais desafiadoras.
- Fóruns dedicados ao aliciamento de crianças estão crescendo em cantos protegidos da Internet, normalizando e incentivando esse comportamento, muitas vezes exigindo 'novo conteúdo' para participar.
- A rápida expansão da Internet está permitindo que os usuários fiquem on-line em áreas que ainda precisam desenvolver/implementar uma estratégia de salvaguarda abrangente ou a infraestrutura relevante.
- As crianças estão usando dispositivos não supervisionadas em idades mais jovens e o comportamento sexual on-line está sendo normalizado. O número de imagens autogeradas de abuso está aumentando a cada ano.

Em foco: Conteúdo autogerado

Crianças e adolescentes podem tirar fotos ou vídeos comprometedores de si mesmos. Embora essa conduta por si só não seja necessariamente ilegal e possa ocorrer como parte do desenvolvimento sexual normal e saudável, há riscos de que qualquer conteúdo possa ser divulgado on-line ou offline para prejudicar crianças ou ser usado como base para extorquir favores. Embora algumas crianças possam ser pressionadas ou coagidas a compartilhar imagens sexuais, outras (em particular adolescentes) podem produzir conteúdo sexual voluntariamente. Isso não significa que eles consentem ou são responsáveis pelo uso exploratório ou abusivo e/ou distribuição dessas imagens.

Sexting foi definido como a "autoprodução de imagens sexuais",¹⁶ ou como a "troca de mensagens ou imagens sexuais" e "a criação, compartilhamento e encaminhamento de imagens sexualmente sugestivas de nudez ou quase nudez por meio de telefones celulares

16 Karen Cooper et al., "Adolescents and Self-Taken Sexual Images: A Review of the Literature," *Computers in Human Behavior* 55 (February 2016): 706-16, <https://doi.org/10.1016/j.chb.2015.10.003>.

e/ou Internet”¹⁷. Sexting é uma forma de conteúdo sexualmente explícito autogerado,¹⁸ e a prática é “notavelmente variada em termos de contexto, significado e intenção”¹⁹.

Embora o sexting seja possivelmente a forma mais comum de conteúdo sexualmente explícito autogerado envolvendo crianças, e muitas vezes feito por e entre adolescentes consentidos que obtêm prazer com a experiência, também existem muitas formas de sexting indesejadas. Isso se refere aos aspectos não consensuais da atividade, como compartilhar ou receber fotos, vídeos ou mensagens sexualmente explícitos indesejados, por exemplo, por pessoas conhecidas ou desconhecidas que tentam fazer contato, pressionar ou aliciar da criança. Sexting também pode ser uma forma de bullying sexual, em que uma criança é pressionada a enviar uma foto a um namorado/namorada/colega que a distribui para uma rede de conhecidos sem o seu consentimento.

Em foco: Cyberbullying

Embora o bullying como fenômeno já aconteça bem antes do surgimento da Internet, a dimensão, o escopo e a continuidade adicionais do bullying cometido on-line podem exacerbar ainda mais o que já é uma experiência perturbadora e muitas vezes prejudicial para suas vítimas. Cyberbullying é definido como dano intencional e repetido infligido por meio do uso de computadores, telefones celulares e outros dispositivos eletrônicos. Muitas vezes ocorre em paralelo ao bullying offline que ocorre na escola ou em outro lugar, pode ter dimensões racistas, religiosas ou sexistas adicionais e pode constituir uma extensão do dano causado offline, como por meio de hacking de conta, propagação de fotos e vídeos on-line e a natureza contínua de mensagens ofensivas e disponibilidade do conteúdo. Geralmente, uma questão social em vez de criminal, as políticas para lidar com o cyber-bullying exigem uma abordagem holística que envolve escolas, famílias e principalmente as próprias crianças.

Em foco: Aliciamento on-line e sextorção

Com os rápidos avanços da tecnologia e o aumento do acesso à Internet e às comunicações digitais experimentados nos últimos anos, inevitavelmente se seguiu um risco elevado de atos criminosos on-line contra crianças. Entre essas formas emergentes de exploração sexual infantil on-line estão o aliciamento e a sextorção de crianças on-line. O aliciamento on-line se refere amplamente ao processo de um adulto fazer amizade e influenciar uma criança (menor de 18 anos), por meio do uso da Internet ou de outras tecnologias digitais, para facilitar o contato ou a interação sexual sem contato com essa criança. Por meio do processo de aliciamento, o agressor tenta obter a obediência da criança para manter o sigilo e evitar a

17 Jessica Ringrose et al., “A Qualitative Study of Children, Young People and ‘Sexting’: A Report Prepared for the NSPCC” (London, UK: National Society for the Prevention of Cruelty to Children, 2012), <http://doi.wiley.com/10.1046/j.1365-2206.1997.00037.x..>

18 UNODC, “Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children” (Vienna: UN, 2015), https://www.unodc.org/documents/Cybercrime/Studyon_the_Effects.pdf.
[3] UNODC, Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children, p.22.

19 Cooper et al., “Adolescents and Self-Taken Sexual Images.”

detecção e a punição²⁰. É importante reconhecer que também existem casos de abuso entre amigos.

A INTERPOL relata que a Internet facilita o aliciamento em virtude de ter um grande número de alvos potenciais facilmente acessíveis e possibilitar que os aliciadores se apresentem de uma forma atraente para a criança. Os criminosos sexuais infantis on-line usam manipulação, coerção e sedução para diminuir as inibições e estimular as crianças a se envolverem em atividades sexuais. O aliciador realiza um processo deliberado de identificação de uma vítima potencial vulnerável, coleta de informações sobre suporte familiar da criança e usa pressão ou vergonha/medo para abusar sexualmente de uma criança. Os aliciadores podem usar pornografia adulta e material de abuso ou exploração infantil para desinibir seus alvos potenciais, apresentando a atividade sexual infantil como natural e normal. A Internet mudou a maneira como as pessoas interagem e redefiniu o conceito de 'amigo'. Um aliciador pode estabelecer uma amizade com uma criança on-line com muita facilidade e rapidez, o que obriga a uma reavaliação das mensagens educacionais tradicionais acerca do "perigo do desconhecido".

O aliciamento on-line foi formalmente reconhecido em um instrumento jurídico internacional em 2007 pela Convenção do Conselho da Europa sobre a Proteção de Crianças contra a Exploração Sexual e o Abuso Sexual (Convenção de Lanzarote). O Artigo 23 criminaliza a "solicitação de crianças para fins sexuais", o que exige que haja uma proposta intencional de encontrar a criança com o objetivo de cometer um crime sexual que é seguido por "atos materiais que levem a tal encontro". Em muitos casos de aliciamento, as crianças são abusadas sexualmente e exploradas on-line - o 'encontro' exigido pela Convenção de Lanzarote e muitas leis nacionais existentes é inteiramente virtual - mas é, no entanto, tão prejudicial para a criança quanto uma reunião física. É fundamental que a criminalização do aliciamento se estenda "aos casos em que o abuso sexual não resulta de uma reunião presencial, mas sim on-line"²¹.

Sextorção²² pode ocorrer como uma característica de aliciamento on-line ou como uma ofensa autônoma. Embora a sextorção possa ocorrer sem o processo de aliciamento on-line, em alguns casos, o aliciamento on-line pode levar à sextorção²³. Sextorção pode ocorrer no contexto de aliciamento on-line, pois um aliciador manipula e exerce influência sobre a criança durante o processo de aliciamento por meio de ameaças, intimidação e coerção para

20 International Centre for Missing & Exploited Children, "On-line Grooming of Children for Sexual Purposes: Model Legislation & Global Review," 1st Edition (International Centre for Missing & Exploited Children, 2017), https://www.icmec.org/wp-content/uploads/2017/09/On-line-Grooming-of-Children_FINAL_9-18-17.pdf.

21 Lanzarote Committee, Committee of the Parties to the Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse, Solicitation of children for sexual purposes through information and communication technologies (grooming), Opinion on Article 23 of the Lanzarote Convention and its explanatory note, Jun. 17, 2015, at <https://edoc.coe.int/enchildren-s-rights/7064-lanzarote-committee-opinion-on-article-23-of-the-lanzarote-convention-and-its-explanatory-note.html> (last visited Nov. 6, 2019).

22 National Center for Missing and Exploited Children (NCMEC), Sextortion, at <http://www.missingkids.com/theissues/on-lineexploitation/sextortion> (last visited Nov. 6, 2019).

23 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, Interagency Working Group in Sexual Exploitation of Children, Luxembourg, Jan. 28, 2016, D.4iii, 27-28, at <http://luxembourgguidelines.org/english-version>.

enviar imagens sexuais de si mesma (conteúdo autogerado)²⁴. Se a vítima não fornecer os favores sexuais solicitados, imagens íntimas adicionais, dinheiro ou outros benefícios, suas imagens podem ser postadas on-line com o propósito de causar humilhação ou sofrimento ou coagir a criança a gerar material sexualmente explícito adicional²⁵.

Sextorção tem sido referida como “agressão sexual virtual” por causa dos efeitos emocionais e psicológicos semelhantes nas vítimas²⁶. Em alguns casos, o abuso é tão traumatizante que as vítimas tentaram se machucar ou cometer suicídio como forma de escapar do abuso.

A Europol observou que a coleta de informações para avaliar a extensão da sextorção que afeta as crianças é desafiadora e pode ser altamente subnotificada²⁷. Além disso, a falta de terminologia e definições comuns para o aliciamento e a sextorção on-line são barreiras para a coleta de dados precisos e uma compreensão do verdadeiro escopo das questões globalmente.

2.6 Crianças com vulnerabilidades

Crianças e jovens podem ser vulneráveis por diversos motivos. Uma pesquisa realizada em 2019 afirmou que “a vida digital de crianças vulneráveis raramente recebe a mesma atenção diferenciada e sensível que a adversidade da ‘vida real’ tende a atrair”. Além disso, o relatório prossegue afirmando que “na melhor das hipóteses, eles [crianças e jovens] recebem o mesmo conselho genérico de segurança on-line que todas as outras crianças e jovens, enquanto a intervenção de um especialista é necessária”.

Três exemplos de vulnerabilidades específicas são: crianças migrantes, crianças com transtorno do espectro do autismo e crianças com deficiência), mas é claro que existem muitos outros.

Crianças migrantes

Crianças e jovens de origem migrante geralmente vêm para um país (ou já vivem lá) com um conjunto específico de experiências e expectativas socioculturais. Embora a tecnologia geralmente seja considerada um facilitador para se conectar e participar, os riscos e oportunidades on-line podem variar muito entre os contextos. Além disso, pesquisas e resultados empíricos mostram uma função vital da mídia digital em geral:

- É importante para orientação (ao viajar para um novo país).
- É uma função central para a apropriação e o conhecimento da sociedade/cultura do país receptor.

24 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, Interagency Working Group in Sexual Exploitation of Children, Luxembourg, Jan. 28, 2016, D.4iii, 27-28, at <http://luxembourgguidelines.org/english-version>.

25 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, Interagency Working Group in Sexual Exploitation of Children, Luxembourg, Jan. 28, 2016, D.4iii, 27-28, at <http://luxembourgguidelines.org/english-version>.

26 Benjamin Wittes et al., “Sextortion: Cybersecurity, Teenagers, and Remote Sexual Assault” (Brookings Institution, May 11, 2016), <https://www.brookings.edu/wp-content/uploads/2016/05/sextortion1-1.pdf>.

27 Europol, “On-line Sexual Coercion and Extortion as a Form of Crime Affecting Children: Law Enforcement Perspective” (European Cybercrime Center, May 2017), https://www.europol.europa.eu/sites/default/files/documents/on-line_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf.

- A mídia social pode desempenhar um papel fundamental na manutenção do contato com a família e os colegas e para acessar informações gerais. Juntamente com os muitos aspectos positivos, a mídia digital também pode trazer desafios para os migrantes, incluindo:
- Infraestrutura - é importante pensar em espaços seguros on-line para que crianças e jovens migrantes possam se beneficiar com privacidade e segurança.
- Recursos - os migrantes gastam a maior parte de seu dinheiro em cartões telefônicos pré-pagos.
- Integração - além de ter acesso à tecnologia, crianças e jovens migrantes também precisam receber uma boa educação digital.

Crianças com Transtorno do Espectro Autista (TEA)

O espectro do autismo resume dois domínios principais no processo de diagnóstico de comportamento DSM-5:

- comportamento restrito e repetitivo ("a necessidade de mesmice");
- dificuldade com comportamentos sociais e comunicativos;
- coocorrência frequente com deficiência intelectual, problemas de linguagem e semelhantes.
- A tecnologia e a Internet oferecem oportunidades infinitas para crianças e jovens aprenderem, se comunicarem e brincarem. No entanto, ao lado desses benefícios, existem muitos riscos aos quais as crianças e jovens com TEA podem estar mais vulneráveis:
- A Internet pode dar a crianças e jovens com autismo oportunidades de socialização e interesses especiais que eles podem não ter off-line.
- Desafios sociais, como a dificuldade em entender as intenções dos outros, podem deixar esse grupo vulnerável a "amigos" com más intenções.
- Os desafios on-line estão frequentemente ligados às características centrais do autismo: orientações concretas e específicas podem melhorar as experiências on-line dos indivíduos, mas os desafios subjacentes permanecem.

Crianças com deficiência

Crianças com deficiência enfrentam riscos on-line das mesmas maneiras que crianças sem deficiência, mas também podem enfrentar riscos específicos relacionados às suas deficiências. Crianças com deficiência frequentemente enfrentam exclusão, estigmatização e barreiras (físicas, econômicas, sociais e de atitude) para participar em suas comunidades. Essas experiências podem contribuir para que uma criança com deficiência busque interações sociais e amizades nos espaços on-line, que podem ser positivos, construir autoestima e criar redes de apoio. No entanto, também pode colocá-los em maior risco de incidentes de aliciamento, solicitação on-line e/ou assédio sexual - pesquisas mostram que crianças que

enfrentam dificuldades off-line e aquelas afetadas por dificuldades psicossociais correm maior risco de tais incidentes²⁸.

Crianças que são vítimas off-line provavelmente serão vítimas on-line. Isso coloca as crianças com deficiência em maior risco on-line, mas, ao mesmo tempo, elas têm uma necessidade maior de estar on-line. Pesquisas mostram que crianças com deficiência têm maior probabilidade de sofrer abuso de qualquer tipo²⁹ e, especificamente, maior probabilidade de sofrer vitimização sexual³⁰. A vitimização pode incluir intimidação, assédio, exclusão e discriminação com base na deficiência real ou observada de uma criança, ou sobre aspectos relacionados à sua deficiência, como a forma como se comporta ou fala, equipamento ou serviços que utiliza.

Os autores de aliciamento, solicitação on-line e/ou assédio sexual contra crianças com deficiência podem incluir não apenas criminosos que visam crianças, mas também aqueles que visam crianças com deficiência. Tais criminosos podem incluir “devotos” - pessoas sem deficiência sexualmente atraídas por pessoas com deficiência (mais comumente amputados e pessoas que usam auxiliares de locomoção), alguns dos quais até mesmo fingem ser deficientes³¹. As ações dessas pessoas podem incluir o download de fotos e vídeos de crianças com deficiência (que são de natureza inócua) e/ou seu compartilhamento por meio de fóruns dedicados ou contas de mídias sociais. As ferramentas de denúncia em fóruns e mídias sociais muitas vezes não têm um caminho direcionado ou apropriado para lidar com tais ações.

Existem preocupações de que o “sharenting” (pais compartilhando informações e fotos de seus filhos on-line) pode violar a privacidade de uma criança, levar ao bullying, causar constrangimento ou ter consequências negativas mais tarde na vida³². Os pais de crianças com deficiência podem compartilhar essas informações em busca de apoio ou conselho, colocando as crianças com deficiência em maior risco de resultados adversos.

Algumas crianças com deficiência podem enfrentar dificuldades no uso, ou até mesmo exclusão de ambientes on-line devido ao design inacessível (por exemplo, aplicativos que não permitem que o tamanho do texto seja aumentado), negação de adaptações solicitadas (por exemplo, software de leitura de tela ou controles de computador adaptáveis), ou a

28 Andrew Schrock et al., “Solicitation, Harassment, and Problematic Content,” Berkman Center for Internet & Society, Harvard University, December 2008, 87, https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF-LitReviewDraft_0.pdf.

29 UNICEF, “State of the World’s Children Report: Children with Disabilities,” 2013, https://www.unicef.org/publications/files/SOWC2013_Exec_Summary_ENG_Lo_Res_24_Apr_2013.pdf.

30 Katrin Mueller-Johnson, Manuel P. Eisner, and Ingrid Obsuth, “Sexual Victimization of Youth with a Physical Disability: An Examination of Prevalence Rates, and Risk and Protective Factors,” *Journal of Interpersonal Violence* 29, no. 17 (November 2014): 3180-3206, <https://doi.org/10.1177/0886260514534529>.

31 Richard L Bruno, “Devotees, Pretenders and Wannabes: Two Cases of Factitious Disability Disorder,” *Sexual and Disability* 15, no. 4 (1997): 18, <https://link.springer.com/content/pdf/10.1023/A:1024769330761.pdf>.

32 UNICEF, “Child Privacy in the Age of Web 2.0 and 3.0: Challenges and Opportunities for Policy,” Innocenti Discussion Paper 2017-03 (UNICEF, Office of Research-Innocenti), accessed January 16, 2020, https://www.unicef-irc.org/publications/pdf/Child_privacy_challenges_opportunities.pdf.

necessidade de suporte apropriado (por exemplo, treinamento em como usar o equipamento, suporte pessoal para navegar nas interações sociais³³).

Em relação ao risco do contrato ou assinatura dos termos e condições, as crianças com deficiência correm maior risco de aceitar termos legais que às vezes nem mesmo os adultos conseguem compreender.

2.7 Percepções das crianças sobre os riscos on-line

Exposição mundial à violência, acesso a conteúdo, bens e serviços inadequados; preocupações com o uso excessivo; questões de proteção de dados e privacidade são os riscos destacados pelas crianças³⁴.

Os adolescentes relatam uma série de preocupações em relação ao seu envolvimento com as tecnologias digitais. Isso inclui questões de segurança on-line comumente discutidas, como medo de interagir com estranhos on-line, acessar conteúdo impróprio ou ser exposto a malware ou vírus - enquanto outros estão relacionados à confiabilidade de seu acesso à tecnologia; intrusão dos pais em suas vidas "privadas" on-line; e suas habilidades de alfabetização digital³⁵.

A pesquisa da EU Kids On-line mostra que a pornografia e o conteúdo violento são as principais preocupações on-line das crianças na Europa. De modo geral, os meninos parecem mais incomodados com a violência, enquanto as meninas estão mais preocupadas com os riscos relacionados ao contato³⁶. A preocupação com os riscos é maior entre as crianças de países de "alto uso e alto risco".

Na América Latina, as consultas com crianças mostraram que a perda de privacidade, a violência e o assédio são as principais preocupações³⁷. As crianças relatam ter sido contatadas por pessoas que não conhecem - este é especialmente o caso quando jogam jogos on-line. Nessas situações, a principal estratégia parece não se envolver e/ou bloquear a pessoa. As meninas são confrontadas com assédio nas redes sociais desde cedo. Elas conseguem navegar por essas formas de violência por conta própria, bloqueando usuários e alterando as configurações de privacidade. O assédio vem de usuários que às vezes não falam espanhol, mas conseguem enviar-lhes imagens, solicitar amizade e comentar em suas postagens. Alguns meninos também relatam ter recebido tais pedidos.

33 Para acessar as diretrizes sobre esses direitos, consulte o Artigo 9 da Convenção sobre os Direitos das Pessoas com Deficiência sobre Acessibilidade e o Artigo 21 sobre Liberdade de expressão e opinião e acesso à informação.

34 Amanda Third et al., "Children's Rights in the Digital Age" (Melbourne: Young and Well Cooperative Research Centre, September 2014), http://www.uws.edu.au/__data/assets/pdf_file/0003/753447/Childrens-rights-in-the-digital-age.pdf.

35 Amanda Third et al., "Young and On-line: Children's Perspectives on Life in the Digital Age," The State of the World's Children 2017 Companion Report (Sydney: Western Sydney University, 2017). O relatório resumiu as opiniões de 490 crianças de 10 a 18 anos, de 26 países diferentes, falando 24 línguas oficiais.

36 Livingstone, S. (2014) EU Kids On-line: Findings, methods, recommendations. LSE, London: EU Kids On-line, <https://lisedesignunit.com/EUKidsOn-line/>.

37 Rede Conectados al Sur, "Hablatam."

Em muitas partes do mundo, as crianças têm uma boa compreensão de alguns dos riscos que enfrentam on-line³⁸. A pesquisa mostrou que a maioria das crianças é capaz de distinguir o cyberbullying das piadas ou provocações on-line, reconhecendo que o cyberbullying tem uma dimensão pública e é projetado para causar danos³⁹.

38 Desde 2016, a UIT realiza consultas dentro da POI com crianças e adultos interessados sobre questões relevantes, como cyberbullying, alfabetização digital e atividades infantis on-line.

39 UNICEF, "Global Kids On-line Comparative Report (2019)."

3 Preparando-se para uma estratégia nacional de proteção on-line infantil

Ao desenvolver uma estratégia nacional de proteção on-line infantil para promover a segurança on-line de crianças e jovens, os governos nacionais e as instituições que formulam políticas precisam identificar as melhores práticas e se envolver com as principais partes interessadas.

As seções a seguir destacam os atores e partes interessadas típicos, juntamente com um esboço de seu papel e responsabilidades potenciais com relação à proteção de crianças on-line.

3.1 Atores e partes interessadas

Os formuladores de políticas podem identificar indivíduos, grupos e organizações adequados que representam cada um desses atores e partes interessadas em sua jurisdição. Apreciar cada uma de suas atividades atuais, planejadas e potenciais é importante em qualquer coordenação nacional e orquestração de estratégias de proteção on-line de crianças.

Crianças e jovens

Em todo o mundo, crianças e jovens demonstraram que podem se adaptar e usar as novas tecnologias com grande facilidade. A Internet está se tornando cada vez mais importante nas escolas e como uma arena onde as crianças podem trabalhar, brincar e se comunicar.

De acordo com o último relatório da ChildFund Alliance, apenas 18,1 por cento das crianças entrevistadas pensam que as pessoas que governam agem para protegê-las. É importante que os formuladores de políticas se envolvam com as crianças a esse respeito, reconhecendo seu direito de serem ouvidas (Art. 12 CDC).

Para poder proteger as crianças, os formuladores de políticas devem padronizar a definição de criança em todos os documentos legais. Uma criança deve ser definida como qualquer pessoa com menos de 18 anos. Isso é consistente com o Artigo 1 da Convenção das Nações Unidas sobre os Direitos da Criança (CNUDC), que afirma que “uma criança significa todo ser humano com menos de 18 anos”. As empresas não devem ser autorizadas a tratar como um adulto qualquer pessoa com menos de 18 anos mas que legalmente é velha o suficiente para consentir com o processamento de dados. Essa definição restrita não é justificada por nenhuma evidência sobre marcos de desenvolvimento infantil. Enfraquece os direitos e ameaça a segurança das crianças.

Embora muitas crianças possam parecer confiantes no uso da tecnologia, muitas se sentem inseguras⁴⁰ on-line e têm várias preocupações⁴¹ em relação à Internet.

A falta de experiência de crianças e jovens no mundo mais amplo pode torná-los vulneráveis a uma série de riscos. Eles têm o direito de esperar ajuda e proteção. Também é importante lembrar que nem todas as crianças e jovens vivenciarão a Internet ou as novas tecnologias

40 ChildFund Alliance, “VIOLENCE AGAINST CHILDREN AS EXPLAINED BY CHILDREN,” Save Voices Big Dreams, 2019, https://childfundalliance.org/zdocs/a9357061-749f-4ebf-a1e9-b1aee81cb216/SVBD-THE_REPORT-digital.pdf.

41 Council of Europe, “It’s Our World: Children’s Views on How to Protect Their Rights in the Digital World,” Report on child consultations (Council of Europe, Children’s Right Division, October 2017), <https://rm.coe.int/it-s-our-world-children-s-views-on-how-to-protect-their-rights-in-the-/1680765dff>.

da mesma forma. Algumas crianças com necessidades especiais causadas por deficiências físicas, ou outros tipos, podem ser particularmente vulneráveis em um ambiente on-line e precisarão de apoio extra.

Pesquisas têm mostrado repetidamente que o que os adultos pensam que as crianças e os jovens estão fazendo on-line e o que realmente está acontecendo pode ser muito diferente. Metade de todas as crianças pesquisadas disse que em seu país os adultos não ouvem sua opinião sobre questões que lhes são importantes⁴². Por esta razão, é importante garantir, em quaisquer arranjos feitos em nível nacional para desenvolver políticas nesta área, que os mecanismos apropriados sejam encontrados para permitir que as vozes de todas as crianças e jovens sejam ouvidas e que suas experiências concretas de uso da tecnologia sejam levadas em consideração.

Pais, responsáveis e educadores

Os pais, tutores e educadores passam uma grande parte do tempo com as crianças. Eles devem ser educados em alfabetização digital para compreender o ambiente on-line e ser capazes de proteger as crianças e ensiná-las a se protegerem.

As instituições educacionais têm a responsabilidade particular de ensinar as crianças sobre como ficar mais seguras on-line, quer estejam usando a Internet na escola, em casa ou em qualquer outro lugar, e os formuladores de políticas devem incluir nos currículos nacionais a alfabetização digital desde uma idade muito cedo (3 a 18 anos). Isso permitiria que as crianças pudessem se proteger, conhecer seus direitos e, portanto, utilizar a Internet como facilitadora de conhecimento⁴³.

Os formuladores de políticas são lembrados de que os pais e responsáveis quase sempre serão a primeira, a última e a melhor linha de defesa e apoio para seus próprios filhos. No entanto, quando se trata da Internet, eles podem se sentir um pouco perdidos. Mais uma vez, as escolas podem funcionar como um canal importante para alcançar os pais e encarregados da educação, para sensibilizá-los sobre os riscos e as muitas possibilidades positivas que as novas tecnologias apresentam. No entanto, as escolas não devem ser o único caminho para chegar aos pais e responsáveis. É importante usar muitos canais diferentes para maximizar a possibilidade de chegar ao maior número possível de pais e responsáveis. A indústria tem um papel significativo aqui no suporte a seus usuários ou clientes. Os pais e responsáveis podem escolher gerenciar a atividade e o acesso on-line de seus filhos, conversar com a criança sobre o comportamento correto e o uso de tecnologias, entender o que a criança está fazendo on-line para que a conversa em família integre as experiências on-line e off-line como uma só.

Os pais e responsáveis também precisam ser um bom exemplo para seus filhos sobre como usar seus dispositivos e se comportar de maneira adequada na Internet.

Os formuladores de políticas devem se lembrar de que os pais e responsáveis devem ser consultados para obter suas opiniões, experiências e compreensão sobre como proteger seus filhos on-line.

42 ChildFund Alliance, "Violence against children as explained by children."

43 UNICEF, "Policy Guide on Children and Digital Connectivity" (Policy Lab, Data, Research and Policy, United Nations Children's Fund, June 2018), <https://www.unicef.org/esa/media/3141/file/PolicyLab-Guide-DigitalConnectivity-Nov.6.18-lowres.pdf>.

Por fim, os formuladores de políticas, juntamente com outras instituições públicas, podem desenvolver campanhas de conscientização pública, inclusive para pais, responsáveis e educadores. As bibliotecas públicas, centros de saúde, até mesmo shoppings e outros grandes centros de varejo podem fornecer locais acessíveis para a apresentação de informações de segurança eletrônica e de habilidades digitais. Ao implementar essa tarefa, os governos devem garantir que haja neutralidade na assessoria prestada, livre de qualquer interesse privado, e cobrindo uma ampla variedade de questões dentro do espaço digital.

Indústria

A indústria é uma das principais partes interessadas no ecossistema, pois o setor possui o conhecimento tecnológico que os formuladores de políticas precisam abordar e compreender a fim de desenvolver a estrutura legal. Portanto, é essencial que os formuladores de políticas envolvam a indústria no processo de elaboração das leis de proteção on-line infantil.

Além disso, é importante incentivar a indústria a incorporar em seus negócios uma abordagem de segurança planejada ao desenvolver novas tecnologias. Claramente, as empresas que estão desenvolvendo ou fornecendo novos produtos e serviços de tecnologia devem ajudar seus usuários a entender como eles funcionam e como usá-los de forma segura e adequada.

A indústria também tem a grande responsabilidade de ajudar a promover a conscientização sobre a agenda on-line e de segurança, especialmente para crianças e seus pais ou responsáveis, mas também para a comunidade em geral. Ao se envolver dessa forma, as partes interessadas do setor aprenderão mais sobre as preocupações de outras partes interessadas e os riscos e danos aos quais os usuários finais estão sendo expostos. Com esse conhecimento, a indústria poderia corrigir os produtos e serviços existentes e identificar os perigos em desenvolvimento.

Avanços recentes em inteligência artificial estão abrindo caminho para que a indústria crie freios e contrapesos muito mais robustos para identificar o usuário e fornecer às crianças um ambiente propício para um comportamento on-line positivo. Esses avanços também podem representar novos riscos para as crianças.

Em alguns países, a Internet é regida por uma estrutura de autorregulação ou co-regulamentação. No entanto, alguns países estão considerando, ou implementaram, estruturas legais e regulamentares, incluindo obrigações para as empresas de detectar, bloquear e/ou remover os danos causados às crianças por plataformas ou serviços, bem como fornecer rotas de relatórios claras e acesso a suporte.

A comunidade de pesquisa e as organizações não governamentais

Dentro das universidades e da comunidade de pesquisa, é muito provável que haja uma variedade de acadêmicos e intelectuais que possuem um interesse profissional e um conhecimento muito detalhado do impacto social e técnico da Internet. Eles são um recurso muito valioso em termos de ajudar os governos nacionais e formuladores de políticas a desenvolver estratégias baseadas em fatos reais e boas evidências. Eles também podem atuar como um contrapeso intelectual aos interesses do mercado que às vezes podem ser de curto prazo e comerciais.

Da mesma forma, dentro da comunidade de organizações não governamentais (ONGs), há uma variedade de conhecimentos e informações que podem ser um recurso inestimável

para alcançar ou fornecer serviços a crianças, pais, responsáveis e educadores para ajudar a promover a agenda de segurança on-line e de forma mais geral, defender o interesse público.

Cumprimento da lei

É um fato triste que, por mais maravilhosa que seja a tecnologia, ela também tenha atraído a atenção de elementos criminosos e anti-sociais. A Internet aumentou muito a circulação de MASI e outros danos on-line. Predadores sexuais têm usado a Internet para fazer contato inicial com crianças, atraindo-as para formas muito prejudiciais de contato, on-line e off-line. O bullying e outras formas de assédio podem causar grandes danos à vida das crianças, e a Internet oferece uma nova maneira de isso acontecer.

Por esses motivos, é essencial que a comunidade responsável por averiguar o cumprimento da lei se envolva totalmente com qualquer estratégia geral para ajudar a tornar a Internet mais segura para crianças e jovens. Os policiais precisam ser devidamente treinados para conduzir investigações de crimes relacionados à Internet contra crianças e jovens. Eles necessitam do nível certo de conhecimento técnico e do acesso a instalações forenses que lhes permitam extrair e interpretar dados obtidos de computadores ou da Internet no menor tempo possível.

Além disso, é muito importante que a aplicação da lei estabeleça mecanismos claros para permitir que crianças e jovens, ou qualquer membro do público, relatem quaisquer incidentes ou preocupações que possam ter sobre a segurança on-line de uma criança ou jovem. Muitos países, por exemplo, estabeleceram linhas diretas para facilitar os relatórios de MASI e semelhantes mecanismos dedicados existem para facilitar os relatórios de outros tipos de questões, por exemplo, bullying. Os formuladores de políticas devem trabalhar com a International Association of Internet Hotlines (INHOPE), apoiando-os na avaliação e processamento de relatórios de MASI e se beneficiando da assistência da INHOPE a organizações em todo o mundo na criação de uma linha direta onde não existe nenhuma. Os formuladores de políticas devem garantir que haja canais de comunicação abertos entre as autoridades policiais e outras partes interessadas. A aplicação da lei é a principal fonte de MASI apreendido dentro das fronteiras nacionais. Um processo deve ser implementado para examinar este material a fim de estabelecer se vítimas locais podem ser identificadas. Quando isso não for possível, o material deve ser passado para a INTERPOL para inclusão no banco de dados da Exploração Sexual Infantil Internacional (ESII). Como se trata de uma ameaça global, os formuladores de políticas precisam garantir a cooperação internacional entre as agências de aplicação da lei em todo o mundo. Isso reduziria o tempo dos processos formais e permitiria aos agentes uma resposta mais rápida.

Serviços sociais

Quando crianças ou jovens são prejudicados ou abusados on-line, por exemplo, por terem uma foto inadequada ou ilegal postada deles, eles provavelmente precisarão de apoio ou aconselhamento especializado e de longo prazo. Também pode haver uma necessidade de envolver os serviços e práticas restaurativas para os infratores, especialmente jovens infratores que também podem ter sido vítimas de abuso on-line ou off-line. Os profissionais que trabalham nos serviços sociais precisarão ser devidamente treinados para poder fornecer esse tipo de apoio. O suporte deve ser feito através de canais on-line e off-line.

Serviços de saúde

O serviço de saúde necessário após qualquer caso de violência contra a criança deve ser coberto pelo plano básico de saúde a nível nacional. As instituições de saúde devem realizar a notificação obrigatória de abusos. Os profissionais de saúde devem estar devidamente equipados e bem informados para poderem apoiar as crianças neste aspecto. Os serviços de saúde devem se estender para incluir o apoio à saúde mental e ao bem-estar das crianças.

Ministérios Governamentais

A política de Proteção On-line Infantil ficará sob a jurisdição de vários Ministérios do Governo e é importante envolver todos eles para qualquer estratégia nacional bem-sucedida e plano de ação. Estas informações podem incluir:

- Assuntos Internos
- Saúde
- Educação
- Justiça
- Informação digital
- Reguladores

Os reguladores estão mais bem posicionados para contribuir com o papel de controlador e contador em colaboração com as instituições governamentais. Isso pode incluir reguladores de proteção de mídia e dados.

Operadores de rede de banda larga, móvel e Wifi

As operadoras podem detectar, bloquear e relatar conteúdo ilegal em sua rede e fornecer ferramentas, serviços e configurações familiares amigáveis para uso dos pais na escolha de como gerenciar o acesso de seus filhos. É importante que os provedores garantam igualmente que as liberdades civis e a privacidade sejam respeitadas.

Direitos da Criança

Instituições independentes de direitos humanos para crianças podem desempenhar um papel crucial para garantir a proteção on-line das crianças. Embora seus mandatos variem, essas instituições muitas vezes têm funções para:

- monitorar o impacto da lei, política e prática na proteção dos direitos da criança;
- promover a implementação de padrões internacionais de direitos humanos em nível nacional;
- investigar violações dos direitos da criança;
- fornecer conhecimentos sobre os direitos da criança aos tribunais;
- assegurar que as opiniões das crianças sejam ouvidas sobre questões relativas aos seus direitos humanos, incluindo o desenvolvimento de leis e políticas relevantes;

- promover a compreensão e conscientização pública sobre os direitos da criança; e
- empreender iniciativas de educação e treinamento em direitos humanos.

É importante incluir a consulta direta às crianças, pois é um direito delas nos termos do artigo 12 da CNUDC. As funções de aconselhamento, investigação, conscientização e educação de instituições independentes de direitos humanos para crianças são todas relevantes para prevenir e responder aos danos que as crianças podem sofrer on-line. Essas instituições devem, portanto, estar no centro do desenvolvimento de uma abordagem abrangente e baseada em direitos para fortalecer as estruturas legais, regulamentares e políticas que regem a proteção infantil on-line, incluindo consulta direta com crianças, como é seu direito nos termos do art. 12 CNUDC.

Recentemente, também houve exemplos de jurisdições que introduziram ou consideraram a introdução de agências estaduais com um mandato específico para apoiar os direitos da criança on-line, incluindo sua proteção contra violência ou dano. Onde tais agências existem, elas também devem estar intimamente associadas aos esforços para fortalecer a resposta à proteção on-line de crianças em nível nacional.

3.2 Respostas existentes para proteção on-line infantil

Diversas iniciativas têm sido desenvolvidas para atuar em nível nacional e internacional em face da crescente importância das TICs na vida das crianças em todo o mundo e dos riscos inerentes aos mais jovens em nossas sociedades.

Modelos nacionais

Em nível nacional, diversas legislações devem ser destacadas como cobrindo aspectos importantes de uma estrutura abrangente de Proteção On-line Infantil. Estas incluem, entre outras:

- Diretiva Relativa aos Serviços de Comunicação Social Audiovisual (AVMSD) (revista em 2018, UE)
- Regulamento Geral sobre a Proteção de Dados (RGPD) (2018, UE)

Tem havido desenvolvimentos inovadores na resposta regulatória e institucional dos Estados membros às ameaças à segurança e ao bem-estar on-line das crianças. Não há uma maneira única de responder ao MASl, cyberbullying e outros danos que as crianças encontram on-line, mas é notável que novas abordagens foram tentadas nos últimos anos:

Código de Design Adequado para a Idade (2019, Reino Unido)

No início de 2019, o Information Commissioners Office publicou propostas para seu “código de design adequado à idade” para promover a proteção on-line infantil. O código proposto centrou-se nos melhores interesses da criança, conforme estabelecido na CNUDC, e definiu várias expectativas para a indústria. Isso inclui medidas robustas de verificação de idade, serviços de localização desativados por padrão para crianças, para que a indústria colete e retenha apenas a quantidade mínima de dados pessoais de crianças, para que os produtos sejam seguros por design e para que as explicações sejam adequadas à idade e acessíveis.

The Harmful Digital Communications Act (revisado em 2017, Nova Zelândia)

A legislação de 2015 tornou o abuso cibernético um crime específico e se concentra em uma ampla gama de danos, desde o bullying virtual até a pornografia de vingança. Tem como objetivo deter, prevenir e diminuir a comunicação digital prejudicial, tornando ilegal a publicação de uma comunicação digital com a intenção de causar sofrimento emocional grave a outra pessoa e estabelece uma série de 10 princípios de comunicação. Ela possibilita que usuários reclamem para uma organização independente se esses princípios forem violados ou solicitar ordens judiciais contra o autor ou o hospedeiro da comunicação se o problema não for resolvido.

The eSafety Commissioner (2015, Austrália)

O eSafety Commissioner é a primeira agência governamental do mundo dedicada especificamente à segurança on-line. Estabelecido em 2015, o eSafety tem uma função legal de liderar, coordenar, educar e aconselhar sobre questões de segurança on-line para garantir que todos os australianos tenham experiências on-line seguras, positivas e fortalecedoras. O eSafety administra esquemas de investigação que se concentram em uma variedade de danos, incluindo cyberbullying contra crianças, abuso baseado em imagens e conteúdo proibido. Tem o poder de investigar e tomar medidas para tratar de reclamações ou denúncias envolvendo esses tipos de danos - incluindo, em alguns casos, o poder de enviar notificações a indivíduos e a serviços on-line para a remoção de material. A par dos seus poderes de investigação, o eSafety adota uma abordagem global da comunidade, que se baseia em iniciativas e intervenções sociais, culturais e tecnológicas. Sua prevenção, proteção e esforços pró-ativos fornecem uma abordagem abrangente para a segurança on-line.

Modelos internacionais

A nível internacional e transnacional, recomendações e normas foram emitidas por diferentes partes interessadas. Essas diretrizes baseiam-se no trabalho dos seguintes esforços:

Diretrizes sobre a implementação do [Protocolo Facultativo à Convenção sobre os Direitos da Criança no que diz respeito à venda de crianças, prostituição infantil e pornografia infantil](#).

Diretrizes do Conselho da Europa para respeitar, proteger e cumprir os direitos da criança no ambiente digital⁴⁴.

As diretrizes são dirigidas a todos os estados membros do Conselho da Europa, com o propósito de auxiliar os estados membros e outras partes interessadas relevantes em seus esforços para adotar uma abordagem estratégica abrangente para maximizar a gama completa de direitos da criança no ambiente digital. Entre os muitos tópicos cobertos estão a proteção de dados pessoais, fornecimento de conteúdo para crianças adaptado às suas capacidades em evolução, linhas de apoio e atendimento, vulnerabilidade e resiliência, bem como o papel e as responsabilidades das empresas. Além disso, as diretrizes conclamam os estados a se envolverem com as crianças, inclusive nos processos de tomada de decisão, para garantir que as políticas nacionais abordem de forma adequada os desenvolvimentos no ambiente digital.

44 Council of Europe (2020), The Digital Environment, <https://www.coe.int/en/web/children/the-digital-environment>. The Council of Europe Guidelines to respect, protect and fulfil the rights of the child in the digital environment is the first such set of standards adopted by an intergovernmental body (CM/Rec, 2018).

As diretrizes estão atualmente disponíveis em 19 idiomas. Serão acompanhadas por uma versão do documento para crianças, bem como um manual para formuladores de políticas, que fornecerá medidas concretas sobre como implementar as diretrizes.

Conselho da Europa - Convenção de Lanzarote

Convenção do Conselho da Europa sobre a Proteção de Crianças contra Exploração Sexual e Abuso Sexual ([Convenção de Lanzarote](#)), que exige que os Estados ofereçam uma resposta holística à violência sexual contra crianças, por meio da “abordagem 4ps”: Prevenção, Proteção, Processamento e Promoção de cooperação nacional e internacional. O funcionamento da Convenção em relação ao meio digital foi esclarecido pelo Comitê das Partes da Convenção sobre a Proteção de Crianças contra a Exploração Sexual e o Abuso Sexual (o “Comitê de Lanzarote”), por meio da adoção de diversos documentos. São eles: uma opinião sobre imagens e/ou vídeos sexualmente sugestivos ou explícitos de crianças gerados, compartilhados e recebidos por crianças (6 de junho de 2019); um Parecer Interpretativo sobre a aplicabilidade da Convenção de Lanzarote a crimes sexuais contra crianças facilitados pelo uso das TICs (12 de maio de 2017); uma Declaração na web aborda a publicidade de material ou imagens de abuso sexual infantil ou quaisquer outros crimes estabelecidos de acordo com a Convenção de Lanzarote (16 de junho de 2016); e um [Parecer sobre o Artigo 23 da Convenção de Lanzarote](#) - Solicitação de crianças para fins sexuais através das tecnologias de informação e comunicação (Aliciamento). O Comitê de Lanzarote acompanha a implementação da Convenção: a sua [2ª ronda de monitorização temática](#) do Comitê centra-se na proteção das crianças contra a exploração sexual e o abuso sexual facilitado pelas TICs: será publicado um relatório sobre a ronda de monitorização em 2020. Em 2019, havia 46 Estados Partes na Convenção, incluindo a Tunísia - o primeiro Estado não membro a aderir.

Outras diretrizes do Conselho da Europa

Outras normas e ferramentas do Conselho da Europa contribuem para um acervo coletivo de um quadro abrangente destinado a todas as partes interessadas. A Convenção do Conselho da Europa sobre [Crime Cibernético](#) contém obrigações para as Partes de criminalizar uma série de crimes relacionados a materiais de abuso sexual infantil: atualmente, ela foi ratificada por 64 Estados Partes. O Conselho da Europa concentra-se, inter alia, em empedrar as crianças e as pessoas ao seu redor para navegar na esfera digital com segurança. Isso é promovido por meio de ferramentas educacionais, incluindo um Manual de Alfabetização na Internet totalmente revisado (2017), um Manual de Educação para a Cidadania Digital (2019) e manuais direcionados aos pais (Paternidade na era digital - Orientação dos pais para a proteção on-line de crianças contra a exploração sexual e abuso sexual (2017); Cidadania digital... e seu filho - O que todo pai precisa saber e fazer (2019). Finalmente, o Conselho da Europa realizou uma pesquisa consultiva com crianças em relação aos seus direitos no ambiente digital - É o nosso mundo: as opiniões das crianças sobre como proteger seus direitos no ambiente digital (2017) e conduziu algumas das primeiras pesquisas consultivas com foco na experiência de crianças com deficiência no meio digital - Dois cliques para frente e um clique para trás: Relatório sobre crianças com deficiência no meio digital (2019).

Relatório de Segurança On-line Infantil

Segurança On-line Infantil: Minimizando o risco de violência, abuso e exploração on-line + Declaração Universal de Segurança on-line infantil⁴⁵.

Recomendações da OCDE sobre a Proteção de Crianças On-line (2012/Revisão 2019-2020) Outras iniciativas nacionais e transnacionais devem ser destacadas como apoiando a cooperação internacional, bem como o esforço nacional para estabelecer estratégias de proteção de crianças on-line. Elas são, por exemplo:

O banco de dados de imagens da Exploração Sexual Infantil Internacional

Gerenciado pela INTERPOL, o banco de dados de imagens de exploração infantil sexual internacional (BD ESII) é uma ferramenta poderosa de inteligência e investigação que permite que investigadores especializados compartilhem dados com colegas em todo o mundo. Disponível através do sistema de comunicações policiais globais seguras da INTERPOL (conhecido como I-247), o BD ESII usa um software sofisticado de comparação de imagens para fazer conexões entre vítimas, abusadores e locais. O BD ESII permite que usuários certificados em países membros acessem o banco de dados em tempo real - usando acervos existentes, carregando novos dados, fazendo a triagem e classificação do material, decifrando, conduzindo análises e se comunicando com outros especialistas em todo o mundo em resposta a consultas relacionadas às investigações de exploração sexual infantil.

A WePROTECT Global Alliance

A WePROTECT Global Alliance (WPGA) é um movimento global que junta a influência, experiência e recursos necessários para transformar a forma como a exploração sexual infantil on-line (ESIO) é tratada em todo o mundo. É uma parceria de governos, empresas globais de tecnologia e organizações da sociedade civil. Sua natureza de múltiplas partes interessadas é única neste campo. A visão da WePROTECT Global Alliance é identificar e proteger mais vítimas, prender mais perpetradores e acabar com a exploração sexual infantil on-line.

A WeProtect Global Alliance compreende uma série de componentes, especificamente um Modelo de Resposta Nacional e uma Resposta Estratégica Global. Mais detalhes podem ser encontrados no Apêndice 3.

Índice de Segurança On-line Infantil de 2020

O Índice de Segurança On-line Infantil de 2020 (ISOI) do DQ Institute é a primeira plataforma analítica em tempo real do mundo para ajudar as nações a monitorar melhor o status da segurança on-line de suas crianças.

O ISOI é baseado em seis pilares que formam a estrutura do ISOI. Os pilares um e dois, Riscos Cibernéticos e Uso Digital Disciplinado, relacionam-se ao uso inteligente da tecnologia digital. Os pilares três e quatro, Competência Digital e Orientação e Educação, estão relacionados ao empoderamento. Os dois últimos pilares estão relacionados à infraestrutura, estes são os pilares da Infraestrutura Social e Conectividade.

45 Broadband Commission for Sustainable Development (2019), The State of Broadband 2019: Broadband as a Foundation for Sustainable Development, https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf.

3.3 Exemplos de respostas a danos on-line

Existem vários exemplos de respostas a danos on-line no Apêndice 4. Esses exemplos abrangem respostas educacionais, legislativas e identificação de danos on-line.

3.4 Benefícios de uma estratégia nacional de proteção on-line infantil

Harmonização das Leis

A adoção por todos os países de uma legislação apropriada contra o uso indevido de TICs para fins criminais ou outros é fundamental para alcançar a segurança cibernética global. Visto que as ameaças podem se originar em qualquer lugar do mundo, os desafios são inerentemente internacionais em escopo e requerem cooperação internacional, assistência investigativa e disposições substantivas e processuais comuns. Portanto, é importante que os países harmonizem seus marcos legais para combater o crime cibernético, proteger as crianças on-line e facilitar a cooperação internacional⁴⁶.

O desenvolvimento de legislação nacional adequada, o quadro jurídico do crime cibernético relacionado e, dentro dessa abordagem, a harmonização em nível internacional é um passo fundamental para o sucesso de qualquer estratégia nacional de proteção on-line infantil. Isso requer, antes de mais nada, as disposições do direito penal substantivo necessário para criminalizar atos como fraude de computador, acesso ilegal, interferência de dados, violações de direitos autorais e MASI, ao mesmo tempo que se toma cuidado para que as crianças não sejam criminalizadas indevidamente. O fato de existirem disposições no código penal aplicáveis a atos semelhantes cometidos no mundo real não significa que elas possam ser aplicadas também a atos cometidos pela Internet. Portanto, uma análise completa das leis nacionais atuais é vital para identificar quaisquer lacunas possíveis. A próxima etapa seria identificar e definir a linguagem legislativa e o material de referência que possam ajudar os países a estabelecer leis harmonizadas de crimes cibernéticos e regras processuais. Esses instrumentos práticos podem ser usados pelos países para a elaboração de uma estrutura legal de segurança cibernética e leis relacionadas. A UIT tem trabalhado com os Estados Membros e as partes interessadas relevantes nessa direção e está contribuindo fortemente para o avanço da harmonização global das leis de crimes cibernéticos.

Dado o ritmo acelerado da inovação tecnológica, a autorregulação e a co-regulação têm sido apresentadas como soluções potenciais para a obsolescência da regulação existente e para o longo processo legislativo. No entanto, para serem eficazes, os reguladores/formuladores de políticas precisam definir claramente certos objetivos e desafios on-line de proteção à criança, colocar em prática um processo de revisão e metodologia claros para avaliar a eficácia da autorregulação e co-regulamentação, e no caso que a autorregulação e a co-regulação não abordam os desafios identificados, inicie um processo legislativo formal para enfrentar esses desafios. Além disso, medidas de autorregulação bem-sucedidas poderiam ser gradualmente adotadas em lei formal dentro do processo legislativo para se tornarem uma barreira legal e evitar uma reversão ou rescisão da adesão a certas iniciativas de autorregulação.

46 Broadband Commission for Sustainable Development (2019)

Coordenação

É provável, em toda a gama de atores e partes interessadas, que já exista uma série de atividades e ações existentes com o objetivo de proteger as crianças on-line, mas que estas ocorreram de forma isolada. Entendê-las é importante para avaliar os esforços existentes no desenvolvimento da estratégia nacional de proteção on-line infantil. A estratégia coordenará e direcionará os esforços por meio da orquestração das atividades existentes e novas.

4 Recomendações para estruturas e implementação

Os governos devem abordar todas as manifestações de violência contra crianças no ambiente digital. No entanto, as medidas tomadas para proteger as crianças no ambiente digital não devem restringir indevidamente o exercício de outros direitos, como o direito à liberdade de expressão, o direito de acesso à informação ou o direito à liberdade de associação. Em vez de restringir a curiosidade natural e o senso de inovação das crianças por medo de encontrar riscos on-line, é fundamental explorar a capacidade das crianças e aumentar sua resiliência enquanto exploram o potencial do ambiente digital.

Em muitos casos, atos de violência contra crianças são cometidos por outras crianças. Em tais situações, os governos devem, na medida do possível, buscar abordagens restaurativas que reparem os danos causados, enquanto evitam a criminalização de crianças. Os governos devem promover o uso de TICs na prevenção e no enfrentamento da violência, como o desenvolvimento de tecnologias e recursos para que as crianças acessem informações, bloqueiem materiais nocivos e relatem casos de violência quando eles ocorrerem⁴⁷.

Para enfrentar a situação global de segurança on-line infantil, os governos devem facilitar a comunicação entre suas entidades relevantes e cooperar abertamente para eliminar os danos às crianças on-line.

4.1 Recomendações de estrutura

4.1.1 Quadro Legal

Os governos devem revisar e, quando necessário, atualizar sua estrutura legal para apoiar a plena realização dos direitos da criança no ambiente digital. Uma estrutura legal abrangente deve abordar medidas preventivas; proibição de todas as formas de violência contra crianças no ambiente digital; fornecimento de soluções eficazes, recuperação e reintegração para lidar com as violações dos direitos das crianças; o estabelecimento de aconselhamento sensível às crianças, relatórios e mecanismos de reclamação; e mecanismos de responsabilização para combater a impunidade⁴⁸.

Sempre que possível, a legislação deve ser neutra em termos de tecnologia, para que a sua aplicabilidade não seja prejudicada por desenvolvimentos tecnológicos futuros⁴⁹.

A implementação efetiva da legislação exige que os governos ponham em prática medidas complementares, incluindo iniciativas de conscientização e mobilização social, esforços e campanhas de educação e capacitação de profissionais que trabalham com e para crianças.

Ao desenvolver uma legislação apropriada, também é importante ter em mente que as crianças não são um grupo homogêneo. Respostas diferentes podem ser necessárias para crianças de

47 Special Representative of the Secretary-General on Violence against Children, Annual Report of the Special Representative of the Secretary-General on Violence against Children to the Human Rights Council, A/HRC/31/20 (January 2016), para. 103 and 104.

48 Special Representative of the Secretary-General on Violence against Children, Releasing children's potential and minimizing risks: ICTs, the Internet and Violence against Children, 2014 (New York: United Nations),

49 Special Representative of the Secretary-General on Violence against Children, Releasing children's potential and minimizing risks: ICTs, the Internet and Violence against Children, 2014 (New York: United Nations),

grupos de diferentes idades, bem como para crianças com necessidades específicas ou que correm maior risco de serem prejudicadas no ou por meio do ambiente digital.

Os governos devem criar um ambiente regulatório, legal, previsível e claro que apoie as empresas e terceiros no cumprimento de suas responsabilidades de salvaguardar os direitos das crianças em todas as suas operações, no país e no exterior⁵⁰.

Os seguintes aspectos serão úteis para os formuladores de políticas na revisão do escopo de quaisquer estruturas legais e provisão do seguinte:

- aliciamento ou outras formas de sedução remota, extorsão ou coerção de crianças para contato sexual ou atividade sexual inadequada;
- assegurar a posse, produção e distribuição de MASI, independentemente da intenção de distribuição;
- assédio, intimidação, abuso ou discurso de ódio on-line;
- material terrorista on-line;
- cibersegurança
- reflexão de que o que é ilegal off-line é igualmente ilegal on-line.

4.1.2 Estruturas políticas e institucionais

Garantir o cumprimento dos direitos da criança no ambiente digital exige que os governos encontrem um equilíbrio entre maximizar os benefícios do uso das TICs pelas crianças e minimizar os riscos associados a eles. Isso pode ser alcançado incluindo medidas para proteger as crianças on-line nos planos nacionais de banda larga⁵¹ e desenvolvendo uma estratégia separada de proteção on-line infantil multifacetada. Essa agenda deve ser totalmente integrada com quaisquer estruturas políticas existentes relevantes para os direitos da criança ou proteção da criança e deve, além disso, complementar as políticas nacionais de proteção da criança, oferecendo uma estrutura específica para todos os riscos e potenciais danos para as crianças, com o objetivo de criar um ambiente digital seguro, inclusivo e empoderador⁵².

Os governos devem estabelecer uma estrutura de coordenação nacional com um mandato claro e autoridade suficiente para coordenar todas as atividades relacionadas aos direitos da criança e mídia digital e TICs em níveis intersetoriais, nacionais, regionais e locais. Os governos devem incluir metas com prazos e um processo transparente para avaliar e monitorar o progresso e devem garantir que os recursos humanos, técnicos e financeiros necessários sejam disponibilizados para a operação eficaz desta estrutura⁵³.

50 Comitê das Nações Unidas sobre os Direitos da Criança, Comentário Geral No. 16, para. 53.

51 The State of the Broadband 2019, Recommendation 5.6, page 78. https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf.

52 Para disposições modelo sobre proteção infantil para planos nacionais de banda larga, consulte o capítulo 10 do Child On-line Safety Report.

53 Special Representative of the Secretary-General on Violence against Children, Annual Report of the Special Representative of the Secretary-General on Violence against Children (December 2014) A/HRC/28/55 and Releasing children's potential and minimizing risks: ICTs, the Internet and Violence against Children, 2014 (New York: United Nations), para. 88.

Os governos devem estabelecer uma plataforma com várias partes interessadas para orientar o desenvolvimento, a implementação e o monitoramento da agenda digital nacional para crianças. Essa plataforma deve reunir representantes dos constituintes mais importantes, incluindo: crianças e jovens; associações de pais/cuidadores; as seções relevantes do governo; os setores de educação, justiça, saúde e assistência social; instituições nacionais de direitos humanos e órgãos reguladores relevantes; sociedade civil; indústria; academia; e associações profissionais relevantes.

4.1.3 Quadro regulatório

Os governos são responsáveis por violações dos direitos das crianças causadas ou contribuídas por empresas comerciais quando não tomaram as medidas necessárias, apropriadas e razoáveis para prevenir e remediar tais violações ou de outra forma colaboraram com ou toleraram as violações⁵⁴.

Os [Princípios Orientadores sobre Empresas e Direitos Humanos](#) prevêm que as empresas devem fornecer mecanismos de reparação e reclamação que sejam legítimos, acessíveis, previsíveis, equitativos, compatíveis com os direitos, transparentes, baseados no diálogo e envolvimento e uma fonte de aprendizagem contínua. Os mecanismos de reclamação estabelecidos por empresas comerciais podem fornecer soluções alternativas flexíveis e oportunas e, às vezes, pode ser do interesse da criança que as questões levantadas sobre a conduta da empresa sejam resolvidas por meio deles. Em todos os casos, deve estar disponível o acesso aos tribunais ou a revisão judicial dos recursos administrativos e outros procedimentos⁵⁵. Deve-se considerar os mecanismos que criam serviços seguros e adequados à idade das crianças para que os usuários relatem suas preocupações.

Não obstante a existência de mecanismos internos de reclamação, os governos devem estabelecer mecanismos de monitoramento para a investigação e reparação de violações dos direitos das crianças, com vista a melhorar a responsabilização das TICs e outras empresas relevantes, bem como fortalecer a responsabilidade da agência reguladora para o desenvolvimento de normas relevantes para direitos da criança e TICs⁵⁶. Isso é especialmente importante porque outros recursos disponíveis para aqueles adversamente afetados por ações corporativas - como processos civis e outras reparações judiciais - costumam ser pesados e caros⁵⁷.

O [Comitê das Nações Unidas sobre os Direitos da Criança](#) destacou o papel potencial das instituições nacionais de direitos humanos nesta área, delineando como elas poderiam ter o papel de receber, investigar e mediar denúncias de violações por entidades da indústria; conduzir inquéritos públicos sobre abusos em grande escala; e realizar revisões legislativas para garantir o cumprimento da Convenção sobre os Direitos da Criança. O Comitê indicou que, quando necessário, "os Estados devem ampliar o mandato legislativo das instituições nacionais de direitos humanos para acomodar os direitos das crianças e os negócios". É

54 Comitê das Nações Unidas sobre os Direitos da Criança, Comentário Geral No. 16, para. 28.

55 Relatório do Representante Especial do Secretário-Geral sobre a questão dos direitos humanos e das empresas transnacionais e outras empresas empresariais, A/HRC/17/31(2011), para. 71.

56 Comitê das Nações Unidas sobre os Direitos da Criança, Relatório do Dia de Discussão Geral de 2014, para. 96.

57 Relatório do Relator Especial sobre a promoção e proteção do direito à liberdade de opinião e expressão, A/HRC/32/38 (2016), para. 71.

especialmente importante que qualquer mecanismo de reclamação seja sensível às crianças, garanta a privacidade e proteção das vítimas e realize atividades de monitoramento, acompanhamento e verificação para as crianças vítimas.

Um exemplo de área em que uma instituição nacional de direitos humanos ou outro órgão regulador poderia oferecer uma solução eficaz para crianças são os casos de cyberbullying. Mecanismos internos de reparação e reclamação às vezes se mostram ineficazes em tais casos porque, embora o conteúdo seja angustiante e prejudicial, muitas vezes não é abordado pela legislação nacional e não há uma base clara para solicitar sua remoção pelo hospedeiro do conteúdo. Capacitar uma autoridade pública para receber reclamações sobre casos de cyberbullying e interceder junto a hospedeiros de conteúdo para que o material relevante seja removido seria uma proteção importante para as crianças⁵⁸. Haveria as vantagens de fornecer uma resposta rápida - que é de importância crucial no contexto do cyberbullying - e também uma base jurídica clara para abordar a remoção do material de cyberbullying.

Ao estruturar sua abordagem para a regulamentação do ambiente digital, os governos também devem estar cientes do impacto de tal regulamentação sobre o gozo de todos os direitos humanos, incluindo a liberdade de expressão⁵⁹.

Os governos devem impor às empresas a obrigação de realizar a devida diligência em relação aos direitos da criança. Isso garantiria que as empresas identificassem, prevenissem e mitigassem seu impacto sobre os direitos das crianças, inclusive em suas relações comerciais e nas operações globais⁶⁰.

Além disso, os governos devem considerar medidas complementares, como garantir que as entidades da indústria cujas atividades possam ter um impacto sobre os direitos das crianças no ambiente digital cumpram os mais altos padrões em termos de prevenção e resposta a potenciais violações de direitos, a fim de se qualificar para financiamento ou contratos.

4.2 Recomendações para implementação

Os governos devem garantir o acesso a recursos eficazes para as crianças vítimas de violações de direitos, incluindo assistência para buscar reparação imediata e apropriada pelos danos sofridos, por meio de compensação quando apropriado. Os governos também devem fornecer apoio e assistência adequados às crianças vítimas de violações relacionadas à mídia digital e às TICs, incluindo serviços abrangentes para garantir a recuperação e reintegração total da criança e prevenir a revitimização de crianças vítimas⁶¹.

Aconselhamento sensível à criança, seguro e facilmente acessível, mecanismos de denúncia e reclamação, como linhas de apoio, devem ser estabelecidos por lei e devem fazer parte do sistema nacional de proteção à criança. É importante garantir que esses serviços estejam conectados a quaisquer serviços regulatórios para ajudar a agilizar as interações da criança com os órgãos institucionais durante um período em que ela possa estar passando por

58 Bertrand de Crombrugghe, "Report of the Human Rights Council on Its Thirty-First Session" (Conselho de Direitos Humanos da ONU, 2016).

59 Relatório do Relator Especial sobre a promoção e proteção do direito à liberdade de opinião e expressão, A/HRC/32/38 (2016), para. 45.

60 Comitê das Nações Unidas sobre os Direitos da Criança, Comentário Geral No. 16, para. 62.

61 Comitê das Nações Unidas sobre os Direitos da Criança, Relatório do Dia de Discussão Geral de 2014, para. 106.

dificuldades. As linhas de apoio são particularmente valiosas no que diz respeito a questões altamente delicadas, como abuso sexual, que as crianças podem achar difícil discutir com colegas, pais, responsáveis ou professores. As linhas de apoio também desempenham um papel crucial no direcionamento de crianças a serviços como serviços jurídicos, casas seguras, aplicação da lei ou reabilitação⁶².

Além disso, os governos precisam entender e rastrear o comportamento do ofensor para aumentar as taxas de detecção de agressores e reduzir o risco de reincidência de agressores condenados. Estabelecer linhas de apoio que oferecem aconselhamento gratuito e anônimo por telefone ou chat e apoio para pessoas que vivenciam sentimentos ou pensamentos de interesse sexual em crianças - infratores em potencial. Ajudar os infratores a mudar seu comportamento minimiza o risco de reincidência.

Os mecanismos legais de tratamento de reclamações também constituem uma parte crucial da estrutura para soluções eficazes.

Os reguladores devem realizar medições e estudos independentes para avaliar como as plataformas relatam e lidam com questões relacionadas à proteção infantil. A tecnologia existe para reguladores monitorarem plataformas de forma independente. Os prestadores de serviços devem ser apoiados para publicar relatórios de transparência.

Junto com a comunidade internacional e a indústria, os governos devem desenvolver um conjunto universal de métricas que as partes interessadas possam usar para medir todos os aspectos relevantes da segurança on-line infantil.

4.2.1 Exploração sexual

Considerações concretas para os formuladores de políticas ao considerar ameaças de danos a crianças, especificamente material de abuso sexual infantil, conteúdo autogerado, aliciamento e sextorção e outros riscos on-line. Ponderando incluir:

- Etapas para interromper ou reduzir o tráfego no MASI, por exemplo, estabelecendo uma linha direta nacional ou um [Portal de Relatórios da IWF](#) implementando medidas que bloquearão o acesso a conteúdo on-line conhecido por conter ou anunciar a disponibilidade de MASI.
- Garantir que os processos nacionais estejam em vigor para garantir que todos os MASI encontrados em um país sejam canalizados para um recurso nacional centralizado com poderes legislativos para direcionar as empresas a remover conteúdo.
- Estratégias para atender à demanda por MASI, especialmente entre aqueles que têm condenações por tais crimes. É importante conscientizar sobre o fato de que este não é um crime sem vítimas: crianças são abusadas para produzir o material que está sendo visualizado e, ao visualizar ou baixar o MASI intencionalmente, uma está contribuindo diretamente para o abuso da criança retratada e outra também está incentivando o abuso de mais crianças para produzir mais fotos.
- Conscientizar sobre o fato de que crianças nunca podem consentir em ser abusadas sexualmente, seja para a produção de MASI ou de qualquer outra forma. Incentivar as pessoas que usam o MASI a buscarem ajuda, ao mesmo tempo, conscientizando-

⁶² Representante Especial do Secretário-Geral para a Violência contra a Criança, Releasing children's potential and minimizing risks, p. 51 and p. 65.

as de que serão criminalmente responsabilizadas pela atividade ilegal na qual se envolveram/estão praticando.

- Outras estratégias para atender à demanda por MASI. Por exemplo, alguns países mantêm um registro de criminosos sexuais condenados. Os tribunais emitiram ordens judiciais proibindo esses infratores de usar totalmente a Internet ou de partes da Internet frequentadas por crianças e jovens. O problema com essas ordens até agora tem sido de execução. No entanto, em alguns países, está sendo considerada a integração da lista de criminosos sexuais conhecidos em uma lista de bloqueio que impedirá aqueles nela de visitar ou ingressar em determinados sites, por exemplo, sites conhecidos por serem visitados por um grande número de crianças e jovens. Obviamente, se o infrator entrar em um site usando um nome diferente ou um login falso, a eficácia de tais medidas pode ser bastante reduzida, mas, ao criminalizar esse comportamento, um novo meio de intimidação pode ser estabelecido.
- Fornecimento de apoio adequado de longo prazo às vítimas. Quando crianças ou jovens foram vítimas on-line, por exemplo, onde uma imagem ilegal deles apareceu na Internet, eles naturalmente se sentirão muito preocupados sobre quem pode ter visto e que impacto isso terá sobre eles. Isso pode fazer com que a criança ou o jovem se sinta vulnerável ao bullying ou a mais exploração e abuso sexual. Nesse contexto, será importante que haja serviços de apoio profissional disponíveis para apoiar as crianças e jovens que se encontram nestas circunstâncias. Esse apoio pode precisar ser fornecido em uma base de longo prazo.
- Assegurar que um mecanismo seja estabelecido e amplamente promovido para fornecer um meio rápido e prontamente entendido para relatar conteúdo ilegal ou comportamento ilegal ou preocupante on-line, por exemplo, um sistema semelhante ao que foi estabelecido pela [Força-Tarefa Global Virtual e INHOPE](#). O uso do sistema INTERPOL i24/7 deve ser incentivado.
- Garantir que um número suficiente de policiais seja devidamente treinado na investigação de crimes na Internet e em computadores e tenha acesso a instalações forenses adequadas para que possam extrair e interpretar dados digitais relevantes.
- Investir no treinamento de autoridades policiais, promotoras e judiciais nos métodos usados por criminosos on-line para cometer esses crimes. Também será necessário investir na aquisição e manutenção das instalações necessárias para obter e interpretar evidências forenses de dispositivos digitais. Além disso, será importante estabelecer colaboração bilateral e multilateral e intercâmbio de informações com as autoridades policiais e órgãos de investigação relevantes em outros países.

4.2.2 Educação

Educar as crianças sobre a alfabetização digital como parte de uma estratégia para garantir que possam se beneficiar da tecnologia, livres de danos. Isso permitirá que as crianças desenvolvam habilidades de pensamento crítico que as ajudarão a identificar e compreender os lados bons e ruins de seu comportamento no espaço digital. Embora seja importante ilustrar para as crianças os danos que podem ocorrer on-line, isso só será eficaz se incluído como parte de um programa de alfabetização digital mais amplo que deve ser adequado à idade e focar nas habilidades e competências. É importante incluir conceitos de aprendizagem social e emocional na educação de segurança on-line, pois eles apoiarão a compreensão e

o gerenciamento das emoções dos alunos para que tenham relacionamentos saudáveis e respeitosos, tanto on-line quanto off-line.

As crianças devem ter ferramentas adequadas e o conhecimento para lidar com a Internet é uma das melhores maneiras de mantê-las seguras. Introduzir a alfabetização digital nos currículos escolares é uma maneira. Outra possibilidade é criar recursos educacionais fora do currículo escolar.

Aqueles que trabalham com crianças devem ter conhecimentos e habilidades adequados para apoiar as crianças com confiança tanto na resposta quanto na solução de problemas relacionados à proteção infantil on-line, bem como fornecer às crianças as habilidades digitais necessárias para se beneficiarem da tecnologia com sucesso.

4.2.3 Indústria

Os participantes da indústria nacional e internacional devem trabalhar para aumentar a conscientização sobre as questões em torno da segurança infantil on-line e ajudar todos os adultos responsáveis pelo bem-estar de uma criança - incluindo pais e cuidadores, escolas, organizações de atendimento a jovens e comunidades - a desenvolver o conhecimento e as habilidades que precisam para manter as crianças seguras. A indústria deve adotar uma abordagem mais segura desde o projeto para seus produtos, serviços e plataformas, reconhecendo a segurança como um objetivo central.

- Fornece ferramentas adequadas à família, adequadas à idade, para ajudar seus usuários a gerenciar melhor a proteção de suas famílias on-line.
- Fornece mecanismos de relatório adequados para que seus usuários relatem problemas e preocupações. Os usuários devem esperar respostas oportunas a esses relatórios com informações sobre as ações tomadas e, se aplicável, onde os usuários podem obter suporte adicional.
- Além disso, fornecer relatórios proativos de abuso contra crianças para detectar e lidar com qualquer tipo de abuso (classificado como atividade criminosa) contra crianças. Essa prática tem mostrado que se todos os stakeholders contribuírem para detectar, bloquear e denunciar, podemos pensar em ter uma Internet mais limpa e segura para todos. A indústria deve considerar a utilização de todas as ferramentas relevantes para evitar que suas plataformas sejam exploradas, como os [Serviços da IWF](#).

É vital envolver todos os atores relevantes no ecossistema, que devem estar cientes dos riscos e danos on-line para evitar que as crianças sejam expostas a riscos desnecessários.

Desenvolver métricas comuns para a segurança on-line infantil para medir todos os aspectos relevantes do assunto. Padrões e métricas comuns são a única maneira de monitorar o progresso nos países e determinar o sucesso dos projetos e atividades implementados para eliminar qualquer violência contra crianças e reconhecer a força do ecossistema de segurança infantil on-line.

5 Desenvolvendo uma estratégia nacional de proteção on-line infantil

5.1 Uma lista de verificação nacional

A fim de formular uma estratégia nacional com foco na segurança on-line infantil, os formuladores de políticas precisam considerar uma série de estratégias.

Tabela 1: Principais áreas a serem consideradas

	#	Principais áreas para consideração	Informação adicional
Quadro legal	1	Rever o quadro existente legal para determinar que todos os poderes necessários legais existem para o cumprimento da lei e outras agências relevantes para proteger pessoas com menos de 18 anos on-line em todas as plataformas da Internet.	Será geralmente necessário que haja um corpo de leis que deixe claro que, qualquer e todo crime que possa ser cometido contra uma criança no mundo real pode, mutatis mutandis, também ser cometido na Internet ou em qualquer outra rede eletrônica. Também possa ser necessário desenvolver novas leis ou adaptar as existentes para proibir certos tipos de comportamento que existem apenas na Internet, como por exemplo a sedução para que crianças realizem ou assistam atos sexuais, ou o aliciamento de crianças para o encontro no mundo real com o intuito sexual.
	2	Estabelecer, mutatis mutandis, que qualquer ato contra uma criança que é ilegal no mundo real também é ilegal no mundo on-line e que a proteção dos dados on-line e as regras de privacidade para crianças também sejam adequadas.	Auxiliar a esses fins, será geralmente necessário que haja um quadro legal que proíba o uso errôneo de computadores para fins criminosos, proibição de hacking ou outros usos maliciosos e não consensuais dos códigos de computadores e que estabeleça que a Internet é um local onde qualquer tipo de crime pode ser cometido.

	#	Principais áreas para consideração	Informação adicional
Quadro regulatório	3	Considerar o desenvolvimento de políticas reguladoras. Isso pode incluir políticas de desenvolvimento regulatórias próprias ou compartilhadas, assim como uma estrutura reguladora completa. O modelo de regulação compartilhado ou próprio pode incluir a formulação e publicação de códigos para a boa prática ou expectativas básicas de segurança on-line, ambos em termos de ajudar a participar, coordenar ou orquestrar e sustentar o envolvimento de todas as partes interessadas relevantes e em termos de aumentar a velocidade com que respostas apropriadas às mudanças tecnológicas possam ser formuladas e colocadas em prática. Um modelo regulatório pode definir as expectativas e obrigações entre as partes interessadas e consagrar-se dentro de um contexto legal. Penalidades para a violação destas políticas podem também ser consideradas.	Alguns países estabeleceram o modelo regulatório próprio ou compartilhado em relação ao desenvolvimento de políticas nesta área e através desses modelos eles publicaram, por exemplo, códigos de boa prática para guiar a indústria da Internet em relação a medidas que podem funcionar melhor quando leva-se em consideração manter crianças e jovens mais seguros on-line. Por exemplo, dentro da União Europeia onde códigos para toda a EU têm sido publicados em sites de redes sociais e em redes de telefones móveis em relação ao fornecimento do conteúdo e os serviços para crianças e jovens através de suas redes. A regulação própria ou compartilhada pode ser mais ágil em termos de melhorar a velocidade com que respostas apropriadas para mudanças tecnológicas podem ser formuladas e colocadas em prática. Mais recentemente diversos países têm desenvolvido e/ou implementado uma estrutura regulatória. Nesses exemplos, a estrutura regulatória emergiu de modelos próprios ou compartilhados e define os requisitos e expectativas para as partes interessadas, em especial para os provedores da indústria, para melhor protegerem seus usuários.

	#	Principais áreas para consideração	Informação adicional
Denunciando - conteúdo ilegal	4	Assegurar que um mecanismo esteja estabelecido e promovido amplamente para proporcionar meios de entendimento fáceis para reportar a variedade de conteúdo ilegal encontrado na Internet. Por exemplo, uma linha direta nacional, com a capacidade de responder rapidamente e remover o material ilegal ou torná-lo inacessível. A indústria deve possuir mecanismos para identificar, bloquear e remover o abuso de crianças on-line, levando todos os serviços relevantes para suas organizações.	Mecanismos para reportar abuso de um serviço on-line ou para reportar o comportamento on-line ilegal ou condenável, por exemplo uma linha direta que deve ser amplamente divulgada e difundida na Internet e em outras mídias. Se uma linha direta nacional não estiver disponível, a IWF oferece uma solução do Reporting Portals. Os links para relatar mecanismos de abuso devem ser exibidos com destaque em partes relevantes de qualquer site que permita a exibição de conteúdo gerado pelo usuário. Também deve ser possível para as pessoas que, de alguma maneira se sentem ameaçadas, ou para pessoas que testemunharam qualquer atividade preocupante na Internet reportarem, o mais rápido possível, às agências aplicadoras da lei relevantes que necessitam ser treinadas e prontas para responder. A Virtual Global Taskforce é um corpo de aplicação da lei que disponibiliza um mecanismo que funciona 24 horas por dia para receber relatórios sobre comportamento ilegal ou conteúdo de pessoas nos EUA, Canadá, Austrália e Itália, com a expectativa de outros países participando em breve. Acesse www.virtualglobaltaskforce.com. Acesse também INHOPE.
Denunciando - preocupações do usuário	5	A indústria deve fornecer aos usuários a oportunidade de reportar preocupações e problemas aos seus usuários e responder de acordo.	Os provedores devem ser obrigados a fornecer, e com sinalizações claras, aos seus usuários a habilidade de relatar problemas e preocupações em seus serviços. Eles devem ser adequados para crianças e prontamente disponíveis.

	#	Principais áreas para consideração	Informação Adicional
Lideranças e Partes Interessadas	6	Envolver todas as partes interessadas relevantes com um interesse na proteção on-line infantil em particular: Agências do governo Aplicação da lei Organizações de serviços sociais Provedores de Serviço de Internet (PSI) e outros Provedores de Serviços Eletrônicos (PSE) Provedores de telefonia móvel Provedores de Wi-Fi público Outras companhias hi-tech relevantes Organizações de professores Organizações de pais e responsáveis Crianças e jovens ONGs de proteção de crianças e outras ONGs relevantes A comunidade acadêmica e de pesquisa Donos de Internet cafés e outros provedores de acesso público, por exemplo, bibliotecas, telecentros, PC Bangs⁶³ e centros de jogos on-line etc.	Muitos governos nacionais têm achado útil mostrar para todas as principais partes interessadas e atores para focarem em desenvolver e implementar uma iniciativa nacional para fazer da Internet um local mais seguro para crianças e jovens, e aumentar a conscientização de problemas e como lidar com eles de maneiras bem práticas. Será importante dentro desta estratégia avaliar que muitos estão constantemente e universalmente conectados à Internet através de diversos dispositivos. Os operadores de banda larga, telefonia móvel e Wi-Fi necessitam estar envolvidos. Adicionalmente, em muitos países a rede de bibliotecas públicas, telecentros e Internet cafés podem ser uma importante fonte de acesso à Internet, particularmente para crianças e jovens.
Pesquisa	7	Empreender pesquisas do espectro dos atores nacionais e partes interessadas para determinar suas opiniões, experiências, preocupações e oportunidades no que diz respeito à proteção on-line infantil. Deve-se também avaliar a extensão de qualquer responsabilidade junto às atividades já existentes ou em planejadas para proteger as crianças on-line.	

	#	Principais áreas para consideração	Informação Adicional
Educação, alfabetização digital e competências	8	Desenvolver recursos de alfabetização digital como parte de qualquer currículo escolar nacional que é apropriado à idade e aplicável para todas as crianças.	As escolas e o sistema educacional geralmente irão representar a base do componente de educação e alfabetização digital de uma estratégia nacional de proteção on-line infantil. Qualquer currículo escolar nacional deve incluir aspectos da proteção on-line infantil e ter como objetivo fornecer crianças de todas as idades com as habilidades para beneficiar-se e usar, com sucesso, a tecnologia e para serem sensíveis em relação as ameaças e danos a serem evitados. Deve também reconhecer e recompensar comportamentos on-line positivos e construtivos. Dentro de qualquer campanha educacional e de conscientização será importante atingir o tom correto. Mensagens baseadas no medo devem ser evitadas e o devido destaque deve ser dado aos recursos positivos e divertidos da nova tecnologia. A Internet tem um grande potencial como meio de empoderar crianças e jovens a descobrirem novos mundos. Ensinar formas positivas e responsáveis de comportamento on-line é o objetivo chave de programas educacionais e de conscientização. Aqueles que trabalham com crianças, especialmente professores, devem estar adequadamente treinados e equipados para educar com sucesso e fornecer às crianças essas habilidades. Eles devem entender as ameaças e danos on-line assim como a habilidade de reconhecer, com propriedade, os sinais de abusos e danos e responder e relatar essas preocupações a fim de proteger suas crianças.

	#	Principais áreas para consideração	Informação Adicional
Recursos educacionais	9	Extraí o conhecimento e experiência de todas as partes interessadas a desenvolver mensagens e materiais seguros para a Internet que refletem as normas culturais locais e leis e garantir que essas sejam distribuídas com eficácia e apropriadamente apresentadas para todas as audiências-chaves. Considerar contar com a ajuda da mídia de massa para promover mensagens de conscientização. Desenvolver materiais que enfatizem os aspectos positivos e empoderadores da Internet para crianças e jovens e evitar mensagens baseadas no medo. Promover formas positivas e responsáveis de comportamento on-line. Considerar desenvolver recursos para ajudar os pais a avaliar a segurança on-line de seus próprios filhos e aprender a minimizar os riscos e maximizar potencial para suas próprias famílias através de uma educação direcionada	Ao produzir materiais educacionais, é importante ter em mente que muitas pessoas que são novas na tecnologia não se sentiram confortáveis para usá-la. Por este motivo, é importante assegurar que materiais de segurança estejam disponíveis seja em forma escrita ou produzidos usando outras mídias com quais os novos usuários se sentiram mais familiarizados como, por exemplo, vídeos. Muitas das grandes empresas da Internet produzem websites que contêm uma grande quantidade de informação sobre as questões on-line para crianças e adolescentes. Apesar disso, frequentemente este material estará disponível em inglês ou em uma quantidade muito limitada de línguas. É importante, então, que materiais sejam produzidos localmente que refletem as leis locais assim como as normas culturais locais. Isso será essencial para qualquer campanha de segurança na Internet ou quaisquer materiais de treinamento que sejam desenvolvidos.
Proteção infantil	10	Assegurar que mecanismos de proteção sistemáticos de crianças estejam em vigor para obrigar todos aqueles que trabalham com crianças (assistentes sociais, saúde, escolas, etc.) a identificar, responder e relatar incidentes de abuso e dano que ocorrem on-line.	

	#	Principais áreas para consideração	Informação Adicional
Conscientização nacional	11	Organizar campanhas de conscientização nacionais para criar oportunidades de ressaltar universalmente as questões de proteção on-line infantil. Pode ser benéfico atrelar campanhas globais, como o Dia da Internet Segura, para formular uma campanha.	Pais, responsáveis e profissionais, como professores, tem um papel crucial a desempenhar para ajudar a manter crianças e jovens mais seguros on-line. Programas de apoio devem ser desenvolvidos, pois ajudam a construir a conscientização das questões e também fornecem estratégias para lidar com os problemas. Deve-se considerar também o uso da ajuda da mídia de massa na divulgação de campanhas e mensagens de conscientização. Oportunidades como o Dia da Internet Segura serão de grande ajuda para estimular e encorajar um diálogo nacional sobre proteção on-line infantil. Muitos países têm conseguido construir campanhas de conscientização nacional com sucesso, usando como base o Dia da Internet Segura, e envolvem a gama completa de atores e partes interessadas na amplificação de mensagens universais na mídia e nas redes sociais.

	#	Principais áreas para consideração	Informação Adicional
Ferramentas, serviços e configurações	12	Considerar a função das configurações dos dispositivos, ferramentas tecnológicas (como programas de filtragem), aplicativos de proteção infantil e configurações que podem ajudar. Encorajar os usuários a serem responsáveis por seus dispositivos, encorajando-os a atualizar o sistema operacional além do uso de programas de segurança e aplicativos adequados.	Há diversos serviços disponíveis que podem ajudar a excluir material indesejado ou bloquear contatos indesejados. Alguns desses programas de segurança infantil e filtragem devem ser essencialmente gratuitos, porque eles são parte de um sistema operacional de computador ou eles são disponibilizados como parte de um pacote disponível de um ISP ou ESP. Os fabricantes de alguns consoles de jogos também disponibilizam ferramentas similar se o aparelho consegue se conectar à Internet. Esses programas não são a prova de golpes, mas eles podem fornecer um nível de suporte bem-vindo, particularmente em famílias com crianças pequenas. A maioria dos dispositivos são fornecidos com configurações que ajudam a proteger as crianças além de promover o uso saudável e balanceado. Isso se estende a mecanismos que permitem que pais gerenciem os dispositivos de seus filhos, alocando tempo, os aplicativos e serviços que eles podem usar e gerenciar suas compras. Mais recentemente relatórios e configurações têm sido desenvolvidos, a fim de que usuários e pais entendam e gerenciem melhor o tempo na frente da tela e o acesso. Essas ferramentas técnicas devem ser usadas como parte de um arsenal mais amplo. O envolvimento dos pais e/ou responsáveis é crítico. Ao se tornarem mais velhas, as crianças irão querer mais privacidade e sentiram um forte desejo de começar a explorar as coisas sozinhas. Além disso, onde existe uma relação de faturamento entre um vendedor e um cliente, os processos de verificação de idade podem atuar de forma efetiva para ajudar vendedores de produtos e serviços com restrição de idade ou os editores de material que se destina a públicos com ou acima de uma certa idade, a chegar a esses públicos específicos. Onde não existe uma relação de faturamento, o uso de tecnologias de verificação de idade pode ser problemático ou em muitos países pode ser impossível devido à falta de fontes de dados confiáveis.

5.2 Exemplos de perguntas

Com a identificação das partes interessadas e atores nacionais, as seguintes perguntas podem ser distribuídas às partes interessadas e atores e convidá-los a preencher e responder. Suas respostas ajudarão a determinar a extensão da cobertura da política, os pontos fortes e também as áreas a serem enfocadas em uma lista de verificação nacional.

- Até que ponto a segurança on-line e os direitos das crianças são da sua responsabilidade?
- Como a segurança on-line e os direitos das crianças estão integrados nas suas políticas e nos seus processos existentes?
- Até que ponto a segurança on-line está coberta pela legislação existente?
- Quais são as suas prioridades de segurança on-line?
- Quais atividades você tem para apoiar a segurança on-line?
- Como você trabalha com outras agências e organizações para melhorar/progredir na segurança on-line?
- As crianças-/pais podem relatar preocupações ou problemas de segurança on-line para você?
- Quais são os seus três principais desafios no mundo on-line?
- Quais são as suas três oportunidades principais no mundo on-line?

Também seria útil realizar pesquisas e compreender a percepção e as experiências das crianças, bem como de seus pais, no que diz respeito à proteção on-line infantil.

6 Material de referência

Segurança on-line infantil: principais documentos e publicações

2020

- ECPAT International, [Sexual Exploitation Of Children In The Middle East And North Africa, 2020](#)
- DQ Institute, [2020 Child On-line Safety Report, 2020](#)
- EU Kids On-line, [EU Kids On-line 2020: Survey results from 19 countries, 2020](#)

2019

- Internet Watch Foundation (IWF), [Annual Report, 2019](#)
- WeProtect Global Alliance, [Global Threat Assessment, 2019](#)
- Broadband Commission / ITU, [Child On-line Safety. Universal Declaration, 2019](#)
- Broadband Commission / ITU, [Child Safety On-line: Minimizing the Risk of Violence, Abuse and Exploitation On-line, 2019](#)
- Global Kids On-line, [Growing up in a connected world, 2019](#)
- [Rethinking the Detection of Child Sexual Abuse Imagery on the Internet](#), in Proceedings of the 2019 World Wide Web Conference, May 13-17, 2019, San Francisco, USA, 2019
- UK Home Office, [On-line Harms White Paper \(UK only\), 2019](#)
- PA Consulting, [A tangled web: rethinking the approach to on-line CSEA, 2019](#)
- UK Information Commissioner Office, [Consultation on Code of Practice to help protect children on-line \(UK only\), 2019](#)
- Global Fund to End Violence against Children, [Disrupting Harm: evidence to understand on-line child sexual exploitation and abuse, 2019](#)
- Global Partnership to End Violence against Children, Safe to Learn [Call for Action, Youth Manifesto, 2019](#)
- UNESCO, [Behind the numbers: Ending school violence and bullying, 2019](#) (includes data on on-line hurtful behaviour and cyber-bullying)
- United Nations Human Rights, [children's rights in relation to the digital environment, 2019](#)
- Australian eSafety Commissioner, [Safety by Design Overview, 2019](#)
- UNICEF, [Why businesses should invest in digital child safety brief, 2019](#)
- U.S. Department of State, [Trafficking in Persons report, 2019](#)

2018

- WeProtect Global Alliance, Global Threat Assessment, 2018
- Child Dignity on the Digital World, Technical Working Group Report, 2018 Council of Europe, [Recommendation CM/Rec\(2018\)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment](#), 2018
- Global Fund to End Violence against Children, [Two years of supporting solutions: results from the Fund's investments](#), 2018
- WeProtect Global Alliance, [Country examples of Model of National Response capabilities and implementation](#), 2018
- INTERPOL and ECPAT International, [Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material](#), 2018
- EUROPOL, [Internet Organized Crime Threat Assessment \(IOCTA\)](#), 2018
- NetClean, [Report about Child Sexual Abuse Cybercrime](#), 2018
- International Centre for Missing & Exploited Children (ICMEC), [Child Sexual Abuse Material: Model Legislation & Global Review](#), 9th Edition, 2018
- International Centre for Missing & Exploited Children (ICMEC), [Studies in Child Protection: Sexual Extortion and Non-Consensual Pornography](#), 2018
- International Association of Internet Hotlines, [INHOPE Report](#), 2018
- Internet Watch Foundation (IWF), [Annual Report](#), 2018
- Thorn, Production and Active Trading of Child Sexual Exploitation Images, 2018
- ITU, [Global Cybersecurity Index](#), 2018
- CSA Centre of Expertise, Interventions for perpetrators of on-line child sexual exploitation - a scoping review and gap analysis, 2018
- NatCen, Behaviour and Characteristics of Perpetrators of On-line-facilitated CSEA - a rapid evidence assessment, 2018
- UNICEF, [Policy guide on children and digital connectivity](#), 2018

2017

- The National Center for Missing & Exploited Children (NCMEC), [The on-line enticement of children: an in-depth analysis of CyberTipline Reports](#), 2017
- 5Rights Foundation, [Digital Childhood, development milestones in digital environment](#), 2017
- Childnet, [DeShame Report](#), 2017
- Canadian Centre for Child Protection, [Survivors' survey](#), 2017
- Internet Watch Foundation (IWF), [Annual Report](#), 2017

- International Centre for Missing & Exploited Children (ICMEC), [Annual Report](#), 2017
- International Centre for Missing & Exploited Children (ICMEC), [On-line Grooming of Children for Sexual Purposes: Model Legislation & Global Review](#), 2017
- Thorn, [Sextortion on-line survey with 2,097 victims of sextortion ages 13 to 25](#), 2017
- UNICEF, [Children in a Digital World](#), 2017
- Western Sydney University, [Young and On-line: Children's Perspectives on Life in Digital Age](#), 2017
- ECPAT International, [Sexual Exploitation of Children in South East Asia](#), 2017

2016

- UNICEF, [Perils and possibilities: growing up on-line](#), 2016
- UNICEF, [Child protection in the digital age: National responses to on-line CSEA in ASEAN](#), 2016
- Centre for Justice and Crime Prevention, [Child On-line Protection in the MENA Region](#), 2016
- ECPAT International, Interagency Working Group on Sexual Exploitation of Children, [Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse \(The Luxembourg Guidelines\)](#), 2016

2015

- WeProtect Global Alliance, [Preventing and Tackling Child Sexual Exploitation and Abuse \(CSEA\): A Model National Response](#), 2015
- NCMEC, [A Global Landscape of Hotlines Combating CSAM](#), 2015
- ITU and UNICEF, [Guidelines for Industry on Child On-line Protection](#), 2015

Sobre direitos humanos em um mundo digital

- Council of Europe, [Guidelines to respect, protect and fulfil the rights of the child in the digital environment](#), 2018
- UNESCO, [Internet Universality Indicators](#), 2019
- Ranking Digital Rights (RDR), [2019 RDR Corporate Accountability Index](#), 2019
- Broadband Commission for Sustainable Development, [The State of the Broadband](#), 2019
- ITU, [Measuring Digital Development](#), 2019
- ITU, [Measuring Information Society Report](#), 2018
- UNICEF, [Children and Digital Marketing Industry Toolkit](#), 2018
- Broadband Commission for Sustainable Development, [Digital health](#), 2017

- Broadband Commission for Sustainable Development, [Digital Skills for life and work](#), 2017
- Broadband Commission for Sustainable Development, [Digital gender divide](#), 2017
- UNICEF, Privacy, protection of personal information and reputation, 2017
- UNICEF, Freedom of expression, association, access to information and participation, 2017
- UNICEF, Access to the Internet and digital literacy, 2017
- UN CRC, [Guidelines on effective protection of children from sexual exploitation](#), 2019

Para obter mais recursos, consulte a lista de recursos adicionais em www.itu-cop-guidelines.com

Apêndice 1: Terminologia

As definições abaixo baseiam-se principalmente em terminologias existentes conforme elaboradas na Convenção dos Direitos da Criança de 1989, bem como pelo grupo de trabalho de interações sobre exploração sexual infantil nas Diretrizes de Terminologia para a Proteção de Crianças contra Exploração Sexual e Abuso Sexual, 2016⁶³ (Diretrizes de Luxemburgo), pela Convenção do Conselho da Europa: Proteção de Crianças contra Exploração Sexual e Abuso Sexual, 2012⁶⁴, bem como pelo relatório da Global Kids On-line de 2019⁶⁵.

Adolescente

Adolescentes são pessoas de 10 a 19 anos. É importante notar que os adolescentes não são um termo vinculativo ao abrigo do direito internacional e os menores de 18 anos são considerados crianças, ao passo que os maiores de 19 anos são considerados adultos, a menos que a maioridade seja atingida mais cedo sob legislação nacional⁶⁶.

Inteligência Artificial (IA)

No sentido mais amplo, o termo se refere indistintamente a sistemas que são pura ficção científica (as chamados IAs “fortes” com uma forma autoconsciente) e sistemas que já são operacionais e capazes de realizar tarefas muito complexas (reconhecimento de rosto ou voz, condução de veículos - esses sistemas são descritos como IAs “fracas” ou “moderadas”)⁶⁷.

Sistemas de IA

Um sistema de IA é um sistema baseado em uma máquina que pode, para um determinado conjunto de objetivos definidos pelo homem, fazer previsões, recomendações ou decisões que influenciam ambientes reais ou virtuais e são projetados para operar com níveis variados de autonomia⁶⁸.

63 “Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse,” 2016, 114, <http://luxembourgguidelines.org/wp-content/uploads/2017/06/Terminology-guidelines-396922-EN.pdf>.

64 Council of Europe, Conseil de l’Europe, and Council of Europe, Protection of Children against Sexual Exploitation and Sexual Abuse: Council of Europe Convention (Strasbourg: Council of Europe Publishing, 2012), https://www.coe.int/t/dg3/children/1in5/Source/Lanzarote%20Convention_EN.pdf.

65 Globalkidson-line.net, “Done Right, Internet Use Can Increase Learning and Skills,” November 2019, <http://globalkidson-line.net/synthesis-report-2019/>.

66 UNICEF and ITU, Guidelines for Industry on Child On-line Protection (itu.int/cop, 2015), https://www.itu.int/en/cop/Documents/bD_Broch_INDUSTRY_0909.pdf.

67 Council of Europe, “What’s AI?,” coe.int, Artificial Intelligence, accessed January 16, 2020, <https://www.coe.int/en/web/artificial-intelligence/what-is-ai>.

68 OECD, “Recommendation of the Council on Artificial Intelligence” (OECD, 2019), <https://webcache.googleusercontent.com/search?q=cache:hTtMv9k1ak8J:https://legalinstruments.oecd.org/api/print%3Fids%3D648%26lang%3Den+&cd=3&hl=en&ct=clnk&gl=ch&client=safari>.

Melhor interesse da criança

Descreve todos os elementos necessários para tomar uma decisão em uma situação específica para uma criança, individualmente, ou um grupo de crianças⁶⁹.

Criança

De acordo com o artigo 1 da Convenção sobre os Direitos da Criança, uma criança é qualquer pessoa menor de 18 anos, a menos que a maioridade seja atingida mais cedo de acordo com a legislação nacional⁷⁰.

Exploração e abuso sexual infantil (EASI)

Descreve todas as formas de exploração sexual e abuso sexual (CDC, 1989, art. 34), por exemplo "(a) o incentivo ou coerção de uma criança para se envolver em qualquer atividade sexual ilegal; (b) O uso exploratório de crianças na prostituição ou em outras práticas sexuais ilegais; (c) O uso exploratório de crianças em apresentações e materiais pornográficos", bem como um "contato sexual que geralmente envolve forçar uma pessoa sem consentimento". A exploração e o abuso sexual de crianças ocorrem cada vez mais através da Internet ou com alguma ligação ao ambiente on-line⁷¹.

Material de abuso sexual infantil (MASI)

A rápida evolução das TICs tem criado novas formas de exploração e abuso sexual infantil on-line, que podem ocorrer virtualmente e não precisam incluir encontros face a face com a criança⁷². Embora muitas jurisdições ainda rotulem imagens e vídeos de abuso sexual infantil como 'pornografia infantil' ou 'imagens indecentes de crianças', essas diretrizes se referem aos assuntos coletivamente como material de abuso sexual infantil (doravante, MASI). Isso está de acordo com as Diretrizes da Comissão de Banda Larga e a Resposta Nacional do Modelo da WePROTECT Global Alliance⁷³. Este termo descreve com mais precisão o conteúdo. A pornografia refere-se a uma indústria legítima e comercializada, e conforme as Diretrizes de Luxemburgo declaram o uso do termo:

"pode (inadvertidamente ou não) contribuir para diminuir a gravidade, banalizar ou mesmo legitimar o que é realmente abuso sexual e/ou exploração sexual de crianças [...] o termo

69 OHCHR, "Convention on the Rights of the Child," accessed January 16, 2020, <https://www.ohchr.org/en/professionalinterest/pages/crc.aspx>.

70 OHCHR; UNICEF e ITU, Guidelines for Industry on Child On-line Protection.

71 "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse."

72 "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse"; UNICEF, "Global Kids On-line Comparative Report (2019)."

73 WePROTECT Global Alliance, "Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response.," 2016, <https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/582ba50bc534a51764e8a4ec/1479255310190/WePROTECT+Global+Alliance+Model+National+Response+Guidance.pdf>; Broadband Commission, "Child On-line Safety: Minimizing the Risk of Violence, Abuse and Exploitation On-line (2019)."

'pornografia infantil' corre o risco de insinuar que os atos são realizados com o consentimento da criança e representam material sexual legítimo"⁷⁴.

O termo MASI se refere a material que representa atos que são sexualmente abusivos e/ou exploradores para uma criança. Isso inclui, mas não está limitado a, material registrando o abuso sexual de crianças por adultos; imagens de crianças incluídas em conduta sexualmente explícita; os órgãos sexuais de crianças quando as imagens são produzidas ou usadas para fins principalmente sexuais.

Crianças e jovens

Descreve todas as pessoas com menos de 18 anos, sendo que crianças, também chamadas de crianças mais novas nas diretrizes, abrangem todas as pessoas com menos de 15 anos e jovens compreendem o grupo de 15 a 18 anos.

Brinquedos conectados

Os brinquedos conectados se conectam à Internet usando tecnologias como Wi-Fi e Bluetooth e normalmente operam em conjunto com aplicativos complementares para permitir brincadeiras interativas para as crianças. De acordo com a Juniper Research, em 2015 o mercado de brinquedos conectados atingiu US\$2,8 bilhões e está previsto que aumente para US\$11 bilhões até 2020. Esses brinquedos coletam e armazenam informações pessoais de crianças, incluindo nomes, geolocalização, endereços, fotografias, áudio e gravações de vídeo⁷⁵.

Cyberbullying, também conhecido como bullying on-line

O direito internacional não define o cyberbullying. Para os fins deste documento, o cyberbullying é descrito como um ato agressivo intencional realizado repetidamente por um grupo ou um indivíduo que usa tecnologia digital e tem como alvo uma vítima que não pode se defender facilmente⁷⁶. Geralmente envolve "o uso de tecnologia digital e da internet para postar informações prejudiciais sobre alguém, compartilhar propositalmente informações privadas, fotos ou vídeos de forma prejudicial, enviar mensagens ameaçadoras ou insultuosas (via e-mail, mensagem instantânea, chat, textos), espalhar boatos e informações falsas sobre a vítima ou excluindo-a propositalmente das comunicações on-line"⁷⁷. Pode envolver comunicações diretas (como bate-papo ou mensagem de texto), semipúblicas (como postar uma mensagem de assédio em uma lista de e-mail) ou públicas (como criar um site dedicado a zombar da vítima).

74 "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse."

75 Jeremy Greenberg, "Dangerous Games: Connected Toys, COPPA, and Bad Security," Georgetown Law Technology Review, December 4, 2017, <https://georgetownlawtechreview.org/dangerous-games-connected-toys-coppa-and-bad-security/GLTR-12-2017/>.

76 Anna Costanza Baldry, Anna Sorrentino, and David P. Farrington, "Cyberbullying and Cybervictimization versus Parental Supervision, Monitoring and Control of Adolescents' On-line Activities," Children and Youth Services Review 96 (January 2019): 302-7, <https://doi.org/10.1016/j.childyouth.2018.11.058>.

77 UNICEF, "Global Kids On-line Comparative Report (2019)"; "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse."

Ódio cibernético, discriminação e extremismo violento

“O ódio cibernético, a discriminação e o extremismo violento são uma forma distinta de violência cibernética, pois visa uma identidade coletiva, em vez de indivíduos [...] muitas vezes pertencentes a raça, orientação sexual, religião, nacionalidade ou status de imigração, sexo/gênero e política”⁷⁸.

Cidadania Digital

Cidadania digital refere-se à capacidade de se envolver de forma positiva, crítica e competente no ambiente digital, valendo-se das habilidades de comunicação e criação eficazes, para praticar formas de participação social que respeitem os direitos humanos e a dignidade por meio do uso responsável da tecnologia⁷⁹.

Alfabetização Digital

Alfabetização digital significa ter as habilidades necessárias para viver, aprender e trabalhar em uma sociedade em que a comunicação e o acesso à informação se dão cada vez mais por meio de tecnologias digitais, como plataformas de Internet, mídias sociais e dispositivos móveis⁸⁰. Isso inclui a comunicação clara, as habilidades técnicas e o pensamento crítico.

Resiliência digital

Este termo descreve a capacidade de uma criança de lidar emocionalmente com encontros prejudiciais on-line. A resiliência digital incluiu ter os recursos emocionais necessários para entender quando a criança está em risco on-line, saber o que fazer para buscar ajuda, aprender com a experiência e se recuperar quando as coisas dão errado⁸¹.

Educadores

Um educador é uma pessoa que trabalha sistematicamente para melhorar a compreensão de outra pessoa sobre um determinado assunto. O papel dos educadores abrange aqueles que ensinam em sala de aula e os educadores mais informais que, por exemplo, aqueles que usam plataformas e serviços de sites de redes sociais para fornecer informações de segurança on-line ou administrar cursos comunitários ou escolares para permitir que crianças e jovens permaneçam seguro on-line.

O trabalho dos educadores varia em função do contexto em que atuam e da faixa etária das crianças e jovens (ou adultos) que procuram educar.

78 UNICEF, “Global Kids On-line Comparative Report (2019).”

79 Council of Europe, “Digital Citizenship and Digital Citizenship Education,” Digital Citizenship Education, accessed January 16, 2020, <https://www.coe.int/en/web/digital-citizenship-education/home>.

80 Western Sydney University-Claire Urbach, “What Is Digital Literacy?,” accessed January 16, 2020, https://www.westernsydney.edu.au/studysmart/home/digital_literacy/what_is_digital_literacy.

81 Dr. Andrew K. Przybylski, et al., “A Shared Responsibility. Building Children’s’ On-line Resilience Report” (ParentZone, University of Oxford and Virgin Media, 2014), <https://parentzone.org.uk/sites/default/files/Building%20On-line%20Resilience%20Report.pdf>.

Aliciamento/aliciamento on-line

Aliciamento/aliciamento on-line conforme definido nas Diretrizes de Luxemburgo, refere-se ao processo de estabelecer/construir um relacionamento com uma criança pessoalmente ou através do uso da Internet ou outras tecnologias digitais para facilitar o contato sexual on-line ou off-line com essa pessoa persuadindo a criança a ter uma relação sexual⁸². Um processo destinado a atrair crianças para um comportamento sexual ou conversas com ou sem o seu conhecimento, ou um processo que envolve a comunicação e socialização entre o agressor e a criança a fim de torná-la mais vulnerável ao abuso sexual. O termo aliciamento não foi definido no direito internacional; algumas jurisdições, incluindo o Canadá, usam o termo 'sedução'.

Tecnologias de Informação e Comunicação (TICs)

As tecnologias de informação e comunicação descrevem todas as tecnologias de informação que enfatizam o aspecto da comunicação. Isso inclui todos os serviços e dispositivos de conexão à Internet, como, entre outros, computadores, laptops, tablets, smartphones, consoles de jogos, televisores e relógios⁸³. Inclui ainda serviços como rádio, bem como, banda larga, hardware de rede e sistemas de satélite, entre outros.

Internet e tecnologias associadas

Agora é possível se conectar à Internet usando uma variedade de dispositivos diferentes, por exemplo, smartphones, tablets, consoles de jogos, TVs e laptops, bem como computadores mais tradicionais. Assim, exceto onde o contexto sugerir o contrário, qualquer referência à Internet deve ser entendida como englobando todos esses métodos diferentes. Para abranger a rica e complexa trama da Internet, 'Internet e tecnologias associadas', 'TIC e indústrias on-line' e 'serviços baseados na Internet' são usados indistintamente.

Aviso e remoção

As operadoras e provedores de serviços às vezes são notificados sobre conteúdo suspeito on-line por clientes, membros do público, organizações policiais ou de linha direta. Os procedimentos de notificação e remoção referem-se aos processos de uma empresa para a remoção rápida ('remoção') de conteúdo ilegal (conteúdo ilegal sendo definido de acordo com a jurisdição) assim que forem informados ('notificação') de sua presença em seus serviços.

On-line gaming

'On-line gaming' é definido como jogar qualquer tipo de jogo digital comercial individual ou multiplayer por meio de qualquer dispositivo conectado à Internet, incluindo consoles dedicados, computadores desktop, laptops, tablets e telefones celulares.

O 'ecossistema de jogos on-line' é definido para incluir assistir outros jogarem videogames por meio de e-sports, streaming ou plataformas de compartilhamento de vídeo, que

82 "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse."

83 UNICEF and ITU, Guidelines for Industry on Child On-line Protection.

normalmente fornecem opções para os espectadores comentarem ou interagirem com os jogadores e outros membros da audiência⁸⁴.

Ferramentas de controle parental

Software que permite aos usuários, normalmente os pais, controlar algumas ou todas as funções de um computador ou outro dispositivo que pode se conectar à Internet. Normalmente, esses programas podem limitar o acesso a determinados tipos ou classes de sites ou serviços on-line. Alguns também fornecem espaço para gerenciamento de tempo, ou seja, o dispositivo pode ser configurado para ter acesso à Internet apenas em determinados horários. Versões mais avançadas podem gravar todos os textos enviados ou recebidos de um dispositivo. Os programas normalmente serão protegidos por senha⁸⁵.

Pais, cuidadores, tutores

Vários sites da Internet referem-se aos pais de forma genérica (como em uma “página dos pais” e referem-se a “controles dos pais”). Portanto, pode ser útil definir as pessoas que idealmente deveriam capacitar os filhos para maximizar as oportunidades disponíveis on-line, certificar-se de que crianças e jovens usem sites da Internet com segurança e responsabilidade e dêem seu consentimento para ter acesso a sites específicos da Internet. Neste documento, o termo “pais” refere-se a qualquer pessoa (excluindo educadores) que tenha a responsabilidade legal por uma criança. A responsabilidade parental varia de país para país, assim como os direitos legais dos pais.

Informações pessoais

O termo descreve informações individualmente identificáveis sobre uma pessoa, que são coletadas on-line. Isso inclui o nome completo, detalhes de contato como endereço residencial e de e-mail, números de telefone, impressões digitais ou material de reconhecimento facial, números de seguro ou qualquer outro fator que permita o contato físico ou on-line ou a localização de uma pessoa. Neste contexto, também se refere a qualquer informação sobre uma criança e seu ambiente que é coletada on-line por provedores de serviços on-line, incluindo brinquedos conectados e a Internet das coisas e qualquer outra tecnologia conectada.

Privacidade

A privacidade é frequentemente medida em termos de compartilhamento de informações pessoais on-line, ter um perfil público nas redes sociais, compartilhar informações com pessoas que conheceram on-line, usar configurações de privacidade, compartilhar senhas com amigos, preocupação com a privacidade⁸⁶.

84 UNICEF, “Child Rights and On-line Gaming: Opportunities & Challenges for Children and the Industry,” DISCUSSION PAPER SERIES: Children’s Rights and Business in a Digital World, 2019, https://www.unicef-irc.org/files/upload/documents/UNICEF_CRBDigitalWorldSeriesOn-line_Gaming.pdf.

85 UNICEF and ITU, Guidelines for Industry on Child On-line Protection.

86 “Children’s On-line Privacy Protection Act,” Pub. L. No. 15 U.S.C. 6501-6505 (1998), <https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim>.

Sexting

Sexting é comumente definido como o envio, recebimento ou troca de conteúdo sexualizado de produção própria, incluindo imagens, mensagens ou vídeos por meio de telefones celulares e/ou da Internet⁸⁷. A criação, distribuição e posse de imagens sexuais de crianças é ilegal na maioria dos países. Se imagens sexuais de crianças forem divulgadas, os adultos não devem vê-las. O compartilhamento de imagens sexuais por um adulto com uma criança é sempre um ato criminoso e que entre crianças pode ocorrer dano e relatórios e ações para remover as imagens compartilhadas podem ser necessárias.

Sextorção ou extorsão sexual de crianças

Sextorção descreve ou extorsão sexual (também conhecida como “coerção e extorsão sexual on-line”)⁸⁸ “chantagem de uma pessoa com a ajuda de imagens autogeradas dessa pessoa para extorquir favores sexuais, dinheiro ou outros benefícios dela sob a ameaça de compartilhar o material sem o consentimento da pessoa retratada (por exemplo, postar imagens nas redes sociais)”⁸⁹.

Internet das coisas (IdC)

A Internet das Coisas representa o próximo passo para a digitalização da sociedade e da economia, onde objetos e pessoas se interligam através de redes de comunicação e informam sobre o seu estado e/ou o ambiente ao redor⁹⁰.

URL

A abreviatura significa ‘localizador uniforme de recursos’, o endereço de uma página da Internet⁹¹.

Realidade virtual

A realidade virtual é o uso da tecnologia do computador para criar o efeito de um mundo tridimensional interativo no qual os objetos têm uma sensação de presença espacial⁹².

Wi-Fi

Wi-Fi (Wireless Fidelity) é o grupo de padrões técnicos que permite a transmissão de dados em redes sem fio⁹³.

87 “Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse.”

88 Europol, “On-line Sexual Coercion and Extortion as a Form of Crime Affecting Children: Law Enforcement Perspective” (European Cybercrime Center, May 2017), https://www.europol.europa.eu/sites/default/files/documents/on-line_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf.

89 “Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse.”

90 Ntantko, The Internet of Things, 1 October 2013, Digital Single Market - European Commission, <https://ec.europa.eu/digital-single-market/en/internet-of-things>.

91 UNICEF and ITU, Guidelines for Industry on Child On-line Protection.

92 NASA, “Virtual Reality,” [nas.nasa.gov](https://www.nasa.gov/Software/VWT/vr.html), accessed January 16, 2020, <https://www.nasa.gov/Software/VWT/vr.html>.

93 Children’s On-line Privacy Protection Act.

Apêndice 2: Contatos ofensivos contra Crianças e jovens

Crianças e jovens podem ser expostos a uma variedade de contatos indesejados ou inadequados na Internet que podem ter consequências terríveis para eles. Parte desse contato pode ser de natureza sexual.

Estudos mostram que 22 por cento foram intimidados⁹⁴, assediados ou perseguidos on-line; 24 por cento receberam comentários sexuais indesejados;⁹⁵ 8 por cento encontraram pessoas na vida real que antes só conheciam on-line⁹⁶. Embora as taxas variem por país e região, esses números demonstram que os riscos são reais⁹⁷. Um estudo da Internet nos Estados Unidos da América⁹⁸ descobriu que 32 por cento dos adolescentes on-line foram contatados por um estranho; desses, 23 por cento disseram que se sentiram assustados e desconfortáveis durante o contato; e 4 por cento receberam solicitações sexuais agressivas.

Os predadores sexuais usam a Internet para contatar crianças e jovens para fins sexuais, geralmente usando uma técnica conhecida como aliciamento, pela qual ganham a confiança da criança apelando para seus interesses. Frequentemente, eles apresentam temas sexuais, fotos e linguagem explícita para dessensibilizar, aumentar a consciência sexual e suavizar a vontade de suas jovens vítimas. Presentes, dinheiro e até bilhetes de transporte são usados para persuadir e atrair a criança ou jovem para um lugar onde o predador possa explorá-lo sexualmente. Esses encontros podem até ser fotografados ou gravados em vídeo. As crianças e os jovens muitas vezes não têm maturidade emocional e auto-estima, o que os torna suscetíveis à manipulação e intimidação. Eles também hesitam em contar aos adultos sobre seus encontros por medo de ficarem constrangidos ou de perderem o acesso à Internet. Em alguns casos, eles são ameaçados por predadores e instruídos a manter o relacionamento em segredo. Os predadores sexuais também aprendem uns com os outros por meio de fóruns na Internet e salas de bate-papo.

94 U-report (2019), <http://www.ureport.in/v2/>.

95 Project deSHAME (2017), https://www.childnet.com/ufiles/Project_deSHAME_Dec_2017_Report.pdf.

96 Lenhardt, A., Anderson, M., Smith, A. (2015), Teens, Technology and Romantic Relationships, <https://www.pewresearch.org/internet/2015/10/01/teens-technology-and-romantic-relationships/>

97 Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011). Risks and safety on the internet: The perspective of European children. Full findings. LSE, London: EU Kids On-line , <http://eprints.lse.ac.uk/33731/>.

98 Amanda Lenhart et al., "The Use of Social Media Gains a Greater Foothold in Teen Life as They Embrace the Conversational Nature of Interactive On-line Media.," Pew Internet and American Life Project, 2007, 44, https://www.pewinternet.org/wp-content/uploads/sites/9/media/Files/Reports/2007/PIP_Teens_Social_Media_Final.pdf.pdf.

Apêndice 3: A WeProtect Global Alliance

O Modelo de Resposta Nacional da WePROTECT

A estratégia da WePROTECT Global Alliance apóia os países a desenvolverem respostas coordenadas de múltiplas partes interessadas para combater a exploração sexual infantil on-line, guiadas por seu Modelo de Resposta Nacional (MRN). O Modelo de Resposta Nacional da WPGA atua como um modelo para a ação nacional. Fornece uma estrutura para os países recorrerem para combater a exploração sexual infantil on-line (ESIO). O modelo se destina a ajudar um país a:

- Avaliar sua resposta atual ao ESIO e identificar lacunas;
- Priorizar esforços nacionais para preencher lacunas;
- Aumentar a compreensão e cooperação internacional.

O Modelo não busca prescrever atividades ou estabelecer uma abordagem única. Seu objetivo é descrever as capacidades necessárias para a proteção eficaz da criança e apoiar os países a desenvolver ou aprimorar suas capacidades existentes. Também lista uma série de capacitadores que, se implementados e eficazes, irão acelerar e melhorar os resultados. O MRN inclui vinte e um recursos, divididos em seis seções: política e governança, justiça criminal, vítima, sociedade, indústria e mídia e comunicações. A WPGA acredita que a ação em todas as seis áreas proporcionará uma resposta nacional completa a esse crime.

O Modelo permitirá que um país - independentemente de seu ponto de partida - identifique quaisquer lacunas nas capacidades e comece a planejar para preencher essas lacunas. Embora os países venham a desenvolver suas próprias abordagens individuais, ao fazê-lo dentro do contexto de uma estrutura comum e de compreensão das capacidades, espera-se que a comunicação e a cooperação entre as partes interessadas em nível nacional e internacional possam ser aprimoradas ainda mais.

A Resposta Estratégica Global da WePROTECT

A Reposta Estratégica Global da WePROTECT (REG) é uma abordagem coordenada para combater a exploração sexual infantil on-line para incluir uma visão global maior, uma harmonização internacional de abordagens nacionais e soluções globais além da resposta nacional liderada. A REG é essencialmente a peça que acompanha o Modelo de Resposta Nacional (MRN); enquanto o MRN está focado nas capacidades necessárias para lidar com a ESIO em nível nacional, a REG está focada em áreas prioritárias para colaboração internacional e capacitação.

A REG inclui seis áreas temáticas, com recursos associados necessários e resultados esperados para cada uma, bem como parceiros que devem trabalhar juntos além das fronteiras para entregá-los.

Política e legislação

O desenvolvimento da vontade política de agir e da legislação para harmonizar de forma eficaz a abordagem de crimes resultará na renovação do compromisso de alto nível em nível nacional e internacional para combater a exploração sexual infantil on-line.

Justiça criminal

O compartilhamento de informações, incluindo acesso compartilhado a bancos de dados internacionais por meio de estruturas formais de compartilhamento de dados combinadas com oficiais e promotores dedicados e treinados, com experiência em exploração sexual infantil on-line, é a melhor maneira de identificar, perseguir e apreender criminosos, inclusive por meio de investigações e condenações conjuntas bem-sucedidas.

Impacto da vítima e serviços

O apoio efetivo e oportuno às vítimas, incluindo a proteção de sua identidade e dando-lhes voz, ajuda a garantir que as vítimas tenham acesso ao apoio de que precisam, quando precisam.

Tecnologia

O uso de soluções técnicas, incluindo inteligência artificial, para detectar, bloquear e prevenir material nocivo, transmissões ao-vivo e aliciamento on-line, que deve incluir ampla e consistente adesão ao setor de tecnologia, permitirá que essas plataformas evitem ser utilizadas como ferramenta para exploração sexual infantil on-line.

Sociedade

Existem vários recursos que funcionam juntos dentro da sociedade em geral para capacitar as crianças a se protegerem da exploração sexual infantil on-line, não importa onde vivam. Ao garantir que o desenvolvimento da cultura digital seja mais seguro por design (ou seja, tenha recursos de segurança integrados) e que haja uma abordagem ética e consistente para o relato da mídia, a exposição a conteúdo ilícito on-line será restrita. Enquanto isso, educação e divulgação para crianças e pais, responsáveis e profissionais, e intervenções direcionadas para criminosos, trabalham para prevenir ou mitigar a ocorrência de exploração sexual infantil on-line.

Pesquisa e visão

Finalmente, as avaliações de ameaças (como a Avaliação Global de Ameaças de 2019), a pesquisa do agressor e o trabalho para entender o trauma de longo prazo da vítima darão ao governo, às autoridades policiais, à sociedade civil, à academia e à indústria uma compreensão clara das ameaças mais recentes.

Apêndice 4: Exemplos de respostas a danos on-line

Os exemplos incluídos aqui são compilados pelos autores e colaboradores das diretrizes para formuladores de políticas da UIT.

Educar crianças contra danos on-line

BBC Own IT App - um aplicativo de bem-estar voltado para crianças de 8 a 13 anos que recebem seu primeiro smartphone. Combinando tecnologia de aprendizado de máquina de última geração para rastrear a atividade das crianças em seus smartphones com a capacidade das crianças de autorrelatar seu estado emocional, ele usa essas informações para fornecer conteúdo personalizado e intervenções para ajudar as crianças a ficarem felizes e saudáveis on-line.

Apresentando conteúdo especialmente encomendado por toda a BBC, o aplicativo fornece materiais e recursos úteis para ajudar os jovens a tirar o máximo proveito do seu tempo on-line e construir hábitos e comportamentos on-line saudáveis, ajudando os jovens e os pais a ter conversas mais construtivas sobre suas experiências on-line. O aplicativo não coleta dados pessoais ou conteúdo gerado pelo usuário, pois todo o aprendizado de máquina é executado no aplicativo/dispositivo do usuário.

Project Evolve - Estrutura educacional de competência digital com recursos completos, identificando as habilidades digitais para cada idade da criança para ajudar os pais e professores a entender as competências que seus filhos devem ter, junto com recursos e atividades que lhes fornecerão as habilidades específicas.

360 degree safe - Uma ferramenta de autoavaliação on-line para escolas que consideram e classificam toda a sua oferta de segurança on-line, fornecendo orientação e suporte para obter padrões definidos.

DQ Institute - Os dados foram coletados de 145.426 crianças e adolescentes em 30 países de 2017-2019 como parte do #DQEveryChild, um movimento de cidadania digital global patrocinado pelo DQ Institute, que começou em Cingapura com o apoio da Singtel e se expandiu rapidamente em colaboração com o Fórum Econômico Mundial para incluir mais de 100 organizações parceiras. Este movimento teve como objetivo empoderar crianças com competências abrangentes de cidadania digital, desde o início de suas vidas digitais, usando o programa de educação e avaliação on-line DQ World. Os dados desse movimento foram usados para criar o **Índice de Segurança Infantil On-line de 2020 (ISOI)**. A estrutura do ISOI avalia e classifica a segurança infantil on-line em 30 países com base em 24 áreas agrupadas em seis pilares que afetam a segurança infantil on-line.

O DQ Pro Family Readiness Package e o DQ World oferecem oportunidades para os pais avaliarem a prontidão digital de seus filhos e, por meio de materiais educacionais, melhorar as competências digitais, como cidadania digital, gerenciamento de tempo de tela, gerenciamento de cyberbullying, gerenciamento de segurança cibernética, empatia digital, gerenciamento de pegada digital, pensamento crítico e gerenciamento de privacidade.

O [kit de ferramentas para escolas eSafety](#) da Austrália é um conjunto de recursos projetado para apoiar as escolas na criação de ambientes on-line mais seguros. O kit de ferramentas reflete uma abordagem multifacetada para a educação em segurança on-line e foi categorizado em quatro elementos, com recursos que:

- preparam escolas para avaliar sua prontidão para lidar com questões de segurança on-line e fornecer sugestões para melhorar suas práticas atuais;
- envolvem toda a comunidade escolar para se comprometer e envolver na criação de um ambiente on-line seguro;
- educam destacando as melhores práticas em educação de segurança on-line e apoiando escolas para desenvolver os recursos de segurança on-line da comunidade escolar;
- respondem a incidentes de forma eficaz, apoiando a segurança e o bem-estar.

A campanha educacional do Escritório de Comunicações Eletrônicas da Polônia (UKE) [I Click Sensible](#) educa crianças e pais sobre como ficar mais seguros on-line e como reconhecer e gerenciar riscos.

O ChildFund Viet Nam estabeleceu a iniciativa [Swipe Safe](#). Este programa educa as crianças sobre os potenciais riscos on-line, como golpes cibernéticos, bullying ou abuso sexual, e apresenta conselhos sobre métodos para se manter seguro.

Relatório da Comissão de Banda Larga sobre [Tecnologia, Banda Larga e Educação: avançando na agenda educação para todos](#), 2013.

Experiência das Crianças On-line: Construindo Entendimento e Ação Global, UNICEF, 2019.

A [pesquisa Global Kids On-line](#) inclui uma riqueza de informações sobre respostas de boas práticas a danos on-line.

Exemplos de envolvimento da indústria

O Australian eSafety Commissioner constrói parcerias sólidas e trabalha com a indústria para capacitar todos os australianos a terem experiências on-line mais seguras e positivas. Um exemplo é o trabalho do eSafety sobre segurança desde o projeto. Como parte da iniciativa, o eSafety conduziu um processo detalhado de consulta com a indústria, órgãos comerciais e organizações responsáveis pela proteção dos usuários, bem como pais, responsáveis e jovens. A iniciativa Safety by Design foi projetada para incentivar e ajudar a indústria a garantir que a segurança do usuário seja incorporada ao design, desenvolvimento e implantação de serviços e plataformas on-line. O eSafety também administra três esquemas de denúncias e reclamações: o esquema de cyberbullying, os esquemas de abuso com base em imagens e o esquema de conteúdo on-line. O eSafety pode direcionar formalmente certos provedores de serviços on-line para remover o conteúdo de seus serviços. Embora os esquemas estejam operando em grande parte como um modelo cooperativo entre o governo e a indústria, os poderes disponíveis para o eSafety para obrigar a remoção de material fornecem uma rede de segurança crítica e levam a indústria a ser proativa na abordagem dos danos on-line.

A empresa Telia assume a responsabilidade de compreender e gerir os impactos negativos da conectividade e de ser totalmente transparente e responsável ao nível do Conselho. Eles

também se preocupam com as crianças e jovens porque reconhecem que são usuários ativos de seus serviços.

O [Escritório de Comunicações Eletrônicas da Polônia \(UKE\)](#) está envolvendo a sociedade civil e as crianças em suas campanhas de advocacia para fazê-los perceber o que estão assinando on-line.

A [Internet Watch Foundation](#) é uma organização parceira que reúne indústria, governo, aplicação da lei e ONGs para eliminar o abuso sexual infantil. Em 2020, a IWF tinha 152 membros em plataformas e serviços de infraestrutura e oferece aos membros uma gama de serviços para evitar a disseminação de imagens criminais em suas plataformas.

Cobertura da legislação

Expressa a vontade política de priorizar a POI, assinando a Declaração Universal de Segurança Infantil On-line (Comissão de Banda Larga).

Regulamentação

[Out of the Shadows: O índice iluminando a resposta ao abuso e exploração sexual infantil](#) (2019) da The Economist Intelligence Unit é a única ferramenta de benchmarking que analisa a resposta dos países ao abuso e exploração sexual infantil, incluindo o espaço digital e a resposta da indústria de TIC a ele.

Identificação de abuso de crianças on-line

A seguir estão exemplos de boas práticas para identificar o abuso de crianças on-line.

INHOPE: A rede INHOPE foi formada em 1999 para combater o MASI on-line em resposta a uma visão compartilhada de uma Internet livre de materiais de abuso sexual infantil. Nos 20 anos de intervenção, o INHOPE cresceu para combater com sucesso o crescimento, a disseminação geográfica e a gravidade do MASI on-line. Hoje, as linhas diretas da INHOPE estão trabalhando em todos os continentes, recebendo relatórios e removendo rapidamente o MASI da Internet e compartilhando dados com as autoridades policiais.

O Microsoft **PhotoDNA** cria hashes de imagens e os compara a um banco de dados de hashes já identificados e confirmados como MASI. Se encontrar uma correspondência, a imagem é bloqueada. No entanto, essa ferramenta não emprega tecnologia de reconhecimento facial, nem pode identificar uma pessoa ou objeto na imagem. Mas, com a invenção do PhotoDNA for Video, as coisas tomaram um novo rumo.

PhotoDNA for Video divide um vídeo em quadros-chave e, essencialmente, cria hashes para essas capturas de tela. Da mesma forma que o PhotoDNA pode corresponder a uma imagem que foi alterada para evitar a detecção, o PhotoDNA para Vídeo pode encontrar conteúdo de exploração sexual infantil que foi editado ou combinado em um vídeo que poderia parecer inofensivo.

A Microsoft lançou uma nova ferramenta para identificar predadores infantis que aliciavam crianças para abusos em bate-papos on-line. O **Project Artemis**, desenvolvido em colaboração com The Meet Group, Roblox, Kik e Thorn, baseia-se na tecnologia patenteada da Microsoft e será disponibilizado gratuitamente via Thorn para empresas de serviço on-line que oferecem uma função de chat. O Project Artemis é uma ferramenta tecnológica que ajuda a alertar os administradores quando qualquer moderação é necessária nas salas de chat. Esta técnica de

detecção de aliciamento será capaz de detectar, abordar e relatar predadores que tentam atrair crianças para fins sexuais.

Thorn desenvolveu anúncios de dissuasão voltados para aqueles que procuram material de abuso sexual infantil, que foram veiculados milhões de vezes em quatro mecanismos de pesquisa em um período de três anos. Além disso, os anúncios obtiveram uma taxa de cliques de 3 por cento de pessoas que procuram ajuda depois de procurar por material explorador.

Thorn's **Safer**, uma ferramenta que pode ser implantada diretamente em uma plataforma de empresa privada para identificar, remover e relatar o MASI.

Thorn **Spotlight**, um software que oferece às autoridades policiais em todos os 50 estados dos Estados Unidos da América e no Canadá a capacidade de acelerar a identificação das vítimas e reduzir o tempo de investigação em mais de 60 por cento.

Geebo, um site de classificados comprometido em manter a exploração sexual fora de sua plataforma, nunca teve um caso envolvendo exploração sexual infantil. Eles conseguem fazer isso em parte por causa de seu processo de pré-seleção.

O **classificador de IA do Google** pode ser usado para detectar material de abuso sexual infantil em redes, serviços e plataformas. Essa ferramenta está disponível gratuitamente por meio da **API de segurança de conteúdo do Google**, que é um kit de ferramentas que aumenta a capacidade de revisar o conteúdo de uma forma que exige que menos pessoas sejam expostas a ele. Essa ferramenta ajudaria os especialistas humanos a revisar o material em uma escala ainda maior e bater de frente com os criminosos, visando imagens que não foram previamente marcadas como material ilegal. Compartilhar essa tecnologia aceleraria a identificação de imagens.

Em 2015, o Google expandiu seu trabalho em hashes, introduzindo a primeira tecnologia de impressão digital e correspondência para vídeos no **YouTube**, que verifica e identifica vídeos enviados que contêm material conhecido de abuso sexual infantil.

Durante o Child Safety Hackathon de 2019, o **Facebook** anunciou o código aberto de duas tecnologias que detectam fotos e vídeos idênticos e quase idênticos. Esses dois algoritmos estão disponíveis no GitHub que permite que sistemas de compartilhamento de hash conversem entre si, tornando os sistemas muito mais poderosos.

A **linha direta da IWF** permanece perpetuamente vigilante, não apenas acompanhando os milhares de relatos de membros do público, que podem ter encontrado imagens de abuso sexual infantil on-line, mas também desempenhando um papel proativo único na busca por esse conteúdo ilegal na web. Ao capacitar as linhas diretas para utilizar suas informações e recursos de foco, mais conteúdo pode ser identificado e removido. Além disso, a IWF está trabalhando continuamente com o Google, a Microsoft e o Facebook e outras empresas para expandir constantemente os limites técnicos. A IWF oferece a solução Reporting Portal, que permite aos usuários da Internet em países e nações sem linhas diretas, relatar imagens e vídeos de suspeita de abuso sexual infantil diretamente para a IWF por meio de uma página personalizada do portal on-line.

A IWF, em colaboração com a **instituição de caridade de apoio às vítimas**, a Marie Collins Foundation, pretende criar uma nova campanha convocando os jovens a relatar quaisquer imagens ou vídeos sexuais autogerados de crianças menores de 18 anos que possam encontrar enquanto navegam on-line.

A **Interpol** criou um banco de dados de imagens e vídeos de Exploração Sexual Infantil Internacional (ESII), que é uma ferramenta de inteligência e investigação que permite a investigadores especializados de mais de 50 países compartilhar dados sobre casos de abuso sexual infantil. Ao analisar o conteúdo digital, visual e de áudio de fotografias e vídeos, os especialistas em identificação de vítimas podem recuperar pistas, identificar qualquer sobreposição de casos e combinar seus esforços para localizar vítimas de abuso sexual infantil. Atualmente, o banco de dados de Exploração Sexual Infantil da Interpol contém mais de 1,5 milhão de imagens e vídeos e ajudou a identificar 19.400 vítimas em todo o mundo.

NetClean ProActive é um software baseado em correspondência de assinatura e outros algoritmos de detecção que detecta automaticamente imagens e vídeos de abuso sexual infantil em ambientes empresariais.

Griffeye Brain usa inteligência artificial para escanear conteúdo não classificado anteriormente, compará-lo com os atributos de conteúdo MASI conhecido e sinalizar itens suspeitos para revisão por um agente.

A **RAINN** criou e opera a National Sexual Assault Hotline em parceria com mais de 1.000 prestadores de serviços locais de denúncias de agressões sexuais em todo o país e opera a DoD Safe Helpline para o Departamento de Defesa. A RAINN também realiza programas para prevenir a violência sexual, ajudar sobreviventes e garantir que os perpetradores sejam levados à justiça.

Safehorizon é uma organização sem fins lucrativos de assistência à vítima que está ao lado de vítimas de violência e abuso na cidade de Nova York desde 1978. A Safehorizon oferece serviços de linha direta para vítimas de violência.

O **Project Arachnid** é uma ferramenta inovadora operada pelo Centro Canadense, para combater a crescente proliferação de material de abuso sexual infantil (MASI) na Internet.

[i] <http://www.oecd.org/internet/bridging-the-digital-gender-divide.pdf>

União
Internacional
de Telecomunicações
Place des Nations
CH-1211 Genebra 20 Suíça

ISBN: 978-92-61-30451-5



Publicado na Suíça
Genebra, 2020
Créditos das fotos: Shutterstock