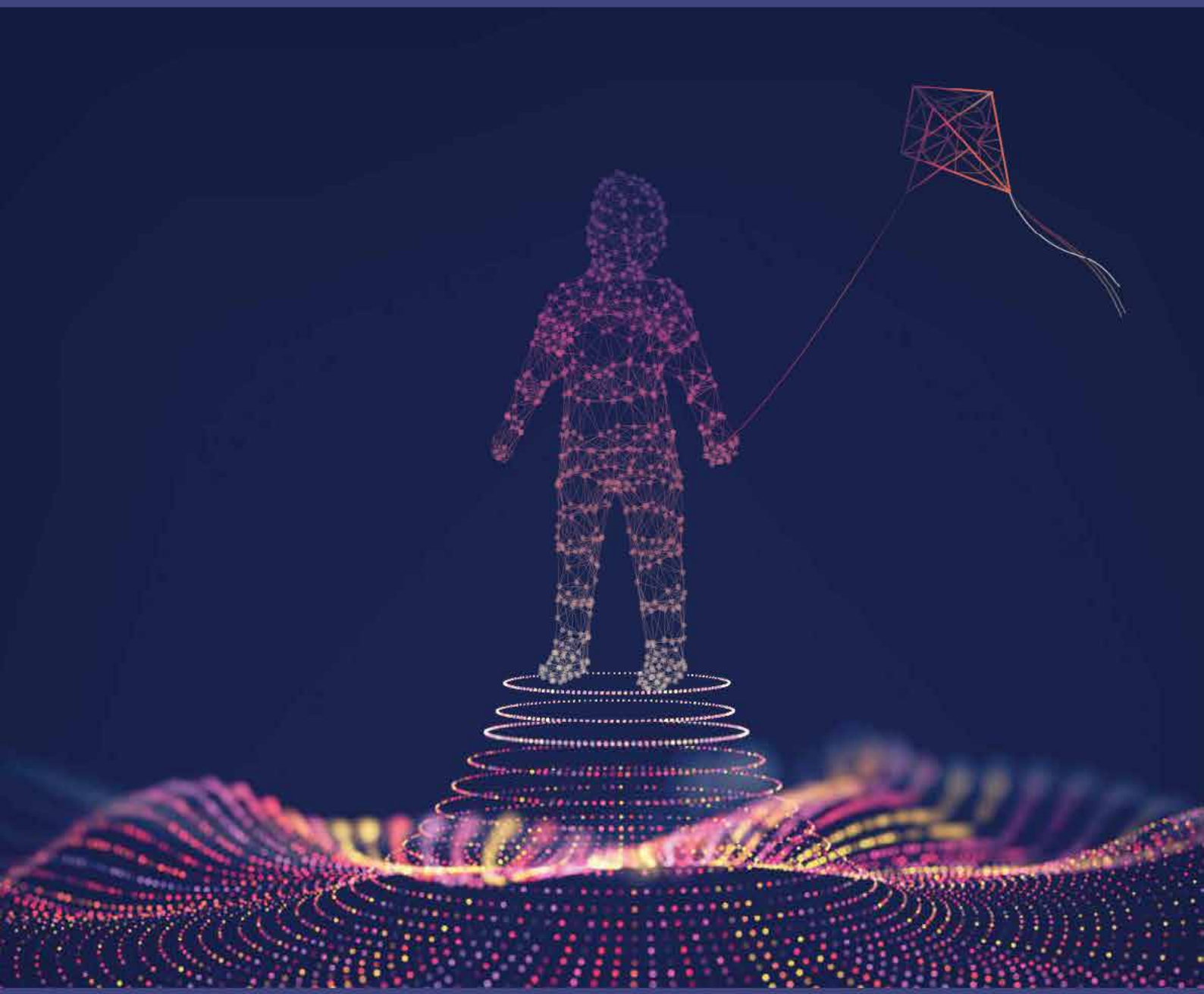


Segurança *online* de crianças e adolescentes:

Minimizar o risco de violência, abuso e exploração sexual *online*

Outubro de 2019

BROADBAND COMMISSION
FOR SUSTAINABLE DEVELOPMENT

Segurança *online* de crianças e adolescentes: minimizar o risco de violência, abuso e exploração sexual *online*

Outubro de 2019

BROADBAND COMMISSION FOR SUSTAINABLE DEVELOPMENT

COMISSÃO DE BANDA LARGA PARA O DESENVOLVIMENTO SUSTENTÁVEL

Publicado em 2020 pela Organização das Nações Unidas para a Educação, a Ciência e a Cultura, 7, place de Fontenoy, 75352 Paris 07 SP, França, e Representação da UNESCO no Brasil e pela Childhood Brasil.

ISBN 978-65-86603-00-2

Título original: *Child Online Safety:* minimizing the risk of violence, abuse and exploitation *online*. Publicado em outubro de 2019 pela Comissão de Banda Larga para o Desenvolvimento Sustentável formada pela Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO) e pela União Internacional de Telecomunicações (UIT).

Coordenação editorial: Childhood Brasil

Coordenação técnica da Representação da UNESCO no Brasil:
Marlova Jovchelovitch Noleto, Diretora e Representante
Adauto Candido Soares, Coordenador do Setor de Comunicação e Informação

Tradução: Montreal Consultants
Revisão técnica: Alessandra Assis e Luiza Britto – Childhood Brasil
Revisão editorial: Unidade de Publicações da Representação da UNESCO no Brasil e Escritório Regional da UIT para as Américas
Diagramação: Lamp Comunicação

Esclarecimento: a UNESCO mantém, no cerne de suas prioridades, a promoção da igualdade de direitos entre homens e mulheres, em todas as suas atividades e ações. Devido à especificidade da língua portuguesa, adotam-se, nesta publicação, os termos no gênero masculino, para facilitar a leitura, considerando as inúmeras menções ao longo do texto. Assim, embora alguns termos sejam escritos no masculino, eles referem-se igualmente ao gênero feminino.

O presente relatório foi elaborado por meio de um processo interativo e colaborativo, com base na *expertise* dos participantes do Grupo de Trabalho sobre Segurança *Online* de Crianças e Adolescentes da Comissão de Banda Larga para o Desenvolvimento Sustentável. O presente Grupo de Trabalho foi criado por iniciativa da Comissão de Banda Larga e consiste em membros da comissão e especialistas externos.

A coordenação dos especialistas externos e o desenvolvimento do conteúdo foram realizadas sob orientação da dra. Joanna Rubinstein (presidente e CEO da World Childhood Foundation dos EUA) e Scott Gegenheimer (CEO do Zain Group). O processo de elaboração do relatório foi facilitado por Doreen Bogdan-Martin (diretora do Setor de Desenvolvimento das Telecomunicações da UIT), Carla Licciardello (ponto focal em Proteção *Online* de Crianças e Adolescentes da UIT) e Anna Polomska (oficial de projetos e analista de políticas) da Secretaria da Comissão de Banda Larga na União Internacional de Telecomunicações (UIT).

Os membros da Comissão de Banda Larga, os pontos focais desses membros e, em particular, os membros do Grupo de Trabalho, realizaram contribuições inestimáveis.

Membros do Grupo de Trabalho

Membros da Comissão de Banda Larga

Sr. Scott GEGENHEIMER (copresidente)
Zain Group

Dra. Joanna RUBINSTEIN (copresidente)
World Childhood Foundation USA

Sra. Audrey AZOULAY (covice-presidente)
UNESCO

Sra. Doreen BOGDAN-MARTIN
Diretora do Setor de Desenvolvimento das Telecomunicações, UIT

Sr. Bocar BA
Samena Telecommunications Council

Dr. Yee-Cheong LEE
ISTIC

Sr. Marcin CICHY
UKE, Poland

Sr. Börje EKHOLM
Ericsson Group

Sra. Kristalina GEORGIEVA
Banco Mundial

Sr. Mats GRANRYD
GSMA

Dr. Carlos M. JARQUE
America Movil

Baronesa Beeban KIDRON
Presidente da 5Rights Foundation

Sr. Adrian LOVETT
Web Foundation

Sua Excelência Sr. Hamad Obaid Al MANSOORI
Emirados Árabes Unidos

Sr. Kevin MARTIN
Facebook

Sr. Paul MITCHELL
Microsoft Corporation

Sr. Sunil Bharti MITTAL
Bharti Enterprises

Dr. Speranza NDEGE
Kenyatta University

Mr. Denis O'BRIEN
Digicel Group

Dr. Abdulaziz Bin Salem AL RUWAIS
Comissão de Comunicações e Tecnologia da Informação, Reino da Arábia Saudita

Sra. Sun YAFANG
Huawei Technologies

Especialistas externos:
Sr. Uri Sadeh
Interpol

Dr. Howard TAYLOR
Parceria Global pelo Fim da Violência contra Crianças e Adolescentes

Sr. John CARR
Consultor independente

Sr. Paul SHAPIRO
ICMEC

Sra. Susie HARTGREAVE
WePROTECT Global Alliance e Internet Watch Foundation

Sr. Robbert VAN DER BERG
ECPAT

Sra. Anna BORGSTROM
NetClean

Dr. Yuhyun PARK
Fórum Econômico Mundial e DQ Institute

Sr. Johan DENNELIND and Ms. Heddy RING
Telia Company

Sr. Amandeep SINGH
UNSG High Level Panel on Digital Cooperation

Sra. Julie CORDUA
Thorn

Sra. Charlotte Petri GORNITZKA e Sra. Jasmine BYRNE
UNICEF

Sra. Elizabeth
LETOURNEAU John Hopkins University

Sr. Ernesto CAFFO
Telefono Azzurro

Sra. Helen MASON
Child Helpline International

Sra. Dushica NAUMOVSKA
INHOPE

Agradecimento especial às pessoas que ajudaram a compilar este relatório:
Sra. Jennifer SULEIMAN
Zain Group

Sra. Lina FERNANDEZ DEL PORTILLO
World Childhood Foundation USA

SUMÁRIO

SUMÁRIO

Prefácio 1

Prefácio da dra. Joanna Rubinstein, Presidente & CEO da World Childhood Foundation EUA, e do sr. Scott Gegenheimer, CEO do Zain Group

Os Objetivos de Desenvolvimento Sustentável (ODS) adotados por todas as nações do mundo em 2015 – e a Convenção sobre os Direitos da Criança, da ONU, que é juridicamente vinculante e que este ano celebra seu 30º aniversário – representam o compromisso global com um futuro melhor para todos, especialmente para crianças e adolescentes; com a nossa próxima geração, de mantê-la saudável, de fornecer a ela acesso à educação, ao entretenimento e a habilidades para assegurar sua empregabilidade futura; e em protegê-los contra qualquer forma de violência, negligência ou tortura. Dar a eles um futuro.

Proteger crianças e adolescentes não é apenas nossa obrigação moral, mas é também um bom negócio apoiar o seu desenvolvimento saudável e feliz. Depende de nós garantir a todos um caminho para um futuro sustentável. Para isso acontecer, adultos – pais, responsáveis, professores, legisladores, o setor privado e outros *stakeholders* – devem garantir que crianças e adolescentes possam atingir seu potencial.

Para tornar esse compromisso uma realidade, a Comissão de Banda Larga para o Desenvolvimento Sustentável criou um Grupo de Trabalho (GT) multissetorial dedicado a abordar a segurança *online* de crianças e adolescentes como um problema global. Esse grupo reuniu representantes sêniores das agências da ONU e de diversas organizações públicas e privadas.

O GT foi encarregado de elaborar um relatório que reunisse as evidências disponíveis sobre a escala e a natureza dos riscos e perigos que crianças e adolescentes enfrentam *online*, bem como fornecer recomendações práticas para a priorização da segurança *online* de crianças e adolescentes.

A conectividade de banda larga é um facilitador chave para o futuro de crianças e adolescentes. Ela ajuda a fomentar a conquista dos ODS e a assegurar que todas as crianças e todos os adolescentes tenham oportunidades iguais de ter sucesso, para que nenhuma criança ou nenhum adolescente fique para trás.

Relatório de segurança *online* de crianças e adolescentes 2019 A internet já tem transformado as nossas vidas em um ritmo e uma escala sem precedentes. Para crianças e adolescentes em países ƒ, o mundo digital é onde nasceram e onde vivem todos os dias. Eles estão se tornando a geração preparada para o 5G e, em última estância, para a 4ª Revolução Industrial, com a Internet das Coisas (IdC), a robótica, a realidade virtual (RV) e a inteligência artificial (IA) mudando nossa forma de viver e trabalhar.

Muitos adultos pensam na internet de uma forma muito instrumental, como algo que eles acessam ou que usam ocasionalmente para realizar coisas específicas. O mesmo não ocorre com crianças e adolescentes. Para uma grande maioria deles, a internet e suas tecnologias associadas estão totalmente integradas em sua forma de viver, entre uma ampla gama de atividades. Elas são, ao mesmo tempo, uma parte e uma extensão de suas vidas: a forma mais importante pela qual eles se comunicam ou se relacionam com deveres de casa, amigos, escola, suas bandas e clubes esportivos favoritos, e até com membros da família.

Ao reconhecer isso, a meta da Comissão de Banda Larga é tornar a conectividade um direito universal e assegurar que todas as crianças e todos os

adolescentes tenham acesso à internet e aos benefícios que ela pode trazer. Como isso se traduz em números? Atualmente, crianças e adolescentes já representam um terço de todos os usuários da internet. Ao mesmo tempo em que se beneficiam imensamente da conectividade para sua educação e seu entretenimento, eles também são expostos a grandes riscos e ameaças *online*, incluindo diferentes formas de violência, como exploração e abuso sexual de crianças e adolescentes, *bullying* e radicalização, entre outros.

Os desafios para se lidar com o lado negativo da conectividade não param de crescer. A menos que ajamos agora, a exploração *online* de crianças e adolescentes pode aumentar a níveis ainda mais assustadores, ao passo em que expandimos a banda larga para os países em desenvolvimento, onde a maioria das crianças e dos adolescentes vivem atualmente. Com frequência, nesses territórios nos quais é recente o processo de digitalização, a infraestrutura educacional e das instituições que aplicam as leis terão dificuldade de se manter atualizadas em relação aos agressores, cada vez mais sofisticados e determinados, que se aproveitam das plataformas e dos serviços digitais. Por isso, elaborar uma abordagem global integrada é mais importante e mais urgente do que nunca.

O presente relatório visa a aumentar a priorização da segurança *online* de crianças e adolescentes entre os principais *stakeholders* e tomadores de decisão de governos, setor privado, sociedade civil, ONGs e universidades. Suas recomendações são práticas e representam uma chamada para a ação coletiva. São baseadas no conhecimento e na *expertise* dos principais grupos especializados que têm um compromisso de longa data e experiência em combater diversas formas de violência *online* contra crianças e adolescentes.

O fato de que 22 membros aderiram ao Grupo de Trabalho é prova do compromisso da Comissão de Banda Larga para o Desenvolvimento Sustentável em priorizar crianças e adolescentes em nossas agendas comuns.

Somos gratos a todos os membros do Grupo de Trabalho, aos membros da Comissão e aos mais de 20 especialistas por sua participação no desenvolvimento deste relatório e por suas recomendações. Esperamos que ajudem a fomentar outras ações para tratar com urgência da segurança *online* de crianças e adolescentes.

Sabemos que é necessária uma comunidade inteira para manter crianças e adolescentes seguros nos ambientes *online* e *offline*. Portanto, contamos com todos os *stakeholders* para priorizar as crianças e os adolescentes e para colaborar e criar ações coletivas para enfrentar e abordar todas as formas de violência, exploração e abuso sexual *online* de crianças e adolescentes *online* (CSEA).

A jornada de crianças e adolescentes pelo mundo digital e sua segurança no mundo real, que estamos todos construindo, são responsabilidades de todos.

Gratos,

Sr. Scott Gegenheimer, CEO do *Zain Group*

Dra. Joanna Rubinstein, Presidente & CEO da *World Childhood Foundation EUA*

Resumo executivo

2

Resumo executivo

Atualmente, a conectividade confiável e acessível está chegando a mais países do que nunca. Ela tem o potencial de transformar a vida de crianças e adolescentes, dando a eles acesso a oportunidades educacionais, culturais e econômicas que antes eram inimagináveis. Porém, com grande frequência, crianças e adolescentes não podem usufruir dessas oportunidades, uma vez que a internet também é um espaço no qual os vulneráveis estão expostos ao risco de sofrer sérios danos.

Em todo o mundo, há mais de 2,2 bilhões de pessoas com menos de 18 anos de idade, o que torna crianças e adolescentes o maior grupo vulnerável em nossas sociedades [1].

Crianças e adolescentes em todo o mundo são expostos de forma regular a riscos e danos *online*, incluindo:

- Abuso, exploração e tráfico sexual – que vai do aliciamento ao estupro, gravado ou exibido pelos agressores.
- Assédio *online*, vitimização e *bullying* cibernético.
- Radicalização e recrutamento por movimentos extremistas.
- Exposição a informações erradas (desinformação) e a conteúdo inadequado, como pornografia ou violência.
- Aplicativos e jogos que são desenvolvidos para incentivar hábitos e comportamentos prejudiciais à saúde.
- Furto e coleta de dados de forma ilegal e não ética.
- Normalização da violência de gênero, por meio da exposição a materiais *online* sobre abuso sexual.

Enfrentar esses perigos e riscos requer uma abordagem global coordenada. Infelizmente, a luta contra a exploração e o abuso sexual de crianças e adolescentes no ambiente *online* não é unificada, nem prosseguida de uma forma consistente entre todos os países. Capacidades, marcos legais, conscientização, falta de recursos alocados e dedicados, e o desejo de agir variam muito entre as agências e os órgãos judiciais dos territórios.

Riscos e perigos *online*

De acordo com pesquisas recentes:

- Em 2018, o Centro Nacional de Crianças e Adolescentes Perdidos e Explorados (*National Center for Missing & Exploited Children* – NCMEC) dos EUA recebeu 18,4 milhões de denúncias de materiais sobre abuso sexual de crianças e adolescentes *online* [2].
- Um estudo recente identificou que 17% dos pais afirmaram que seus filhos já foram vítimas de *bullying* cibernético. Em alguns países, esse número chegou a 37% [3].
- De acordo com o Relatório de Impacto do Instituto DQ de 2017, 56% de crianças e adolescentes entre 8 e 12 anos de idade em 29 países foram expostos a um tempo excessivo na frente da tela e a pelo menos um risco cibernético: incluindo *bullying* cibernético, vício em *videogames*, comportamentos sexuais e encontros *offline* [4].
- Uma em cada cinco crianças e adolescentes entre 9 e 17 anos vê material sexual indesejado *online*, e 25% deles relataram sentir medo ou angústia extremos [5].
- Um estudo de 2019 identificou que 99% dos termos e condições de uso *online* foram escritos com uma linguagem muito complexa para o entendimento de crianças e adolescentes [6].
- De 2016 a 2018, o número de imagens e vídeos ilegais, confirmado pela Linha de Atendimento pela Internet da *International Association of Internet Hotlines* (INHOPE), aumentou 83%.*
- A INHOPE também relatou que a prevalência de crianças e pré-adolescentes (3-13 anos) retratados em imagens e vídeos de exploração e abuso sexual aumentou de 56% de todo o material ilegal (122.276), em 2016, para 79% (148.041), em 2017, e 89% (223.999), em 2018.*

*Relatório Anual da INHOPE 2018. Disponível em: <http://88.208.218.79/Libraries/IC-CAM_IHRMS/INHOPE_Statistics_Report_2018.sflb.ashx>

A Organização Mundial da Saúde (OMS) estima que, a cada ano, 200 milhões de crianças e adolescentes são abusados sexualmente [7]. Além disso, cada vez mais, grande parte desse tipo de violência ocorre *online* ou é obtida e distribuída digitalmente. Nesse caso, a internet é uma facilitadora da exploração e do abuso sexual.

Dentre os problemas que atualmente dificultam a luta contra a violência e todas as outras formas de violações *online* a crianças e adolescentes, alguns dos mais sérios são:

- A inconsistência da legislação entre diferentes territórios, com alguns destes carecendo de leis que abordem especificamente os crimes de abuso sexual contra crianças e adolescentes cometidos *online*.

- A falta de leis e regulamentos que responsabilizem os prestadores de serviço por materiais de abuso sexual de crianças e adolescentes armazenados em suas plataformas.
- A falta de normas e definições comuns e de modalidades colaborativas através das fronteiras, o que dificulta a mensuração da extensão do problema, ou a cooperação integral para lidar com ele.
- Muitos países carecem de capacidade, competência ou infraestrutura para envolver todos os setores cuja cooperação é necessária se quisermos eliminar as violações de crianças e adolescentes no ambiente *online*.
- A falta de dados e pesquisas que abranjam o problema no âmbito global (mesmo neste relatório, muitos dos dados estatísticos que usamos são – por necessidade – do Hemisfério Norte).
- A natureza geralmente sem moderação dos espaços nos quais crianças e adolescentes passam tempo *online* (mídias sociais, plataformas de mensagens, aplicativos de *streaming* em tempo real, espaços virtuais, jogos interativos etc.).
- A dificuldade de monitorar o tráfego da internet, somada à evolução das novas tecnologias, como *smartphones* com preços acessíveis, equipados com câmeras e vídeo de alta resolução, mensagens com fotos, *streaming* em tempo real e criptografia – tudo isso torna ainda mais difícil impedir o abuso sexual de crianças e adolescentes no ambiente *online*.
- As tecnologias digitais geralmente são desenvolvidas com pouca ou nenhuma consideração quanto às formas pelas quais elas podem ser utilizadas para explorar ou abusar sexualmente de crianças ou adolescentes.
- O surgimento do uso e do consumo de tecnologias desenvolvidas para detectar e impedir violações de direitos, como a violência sexual no ambiente *online*, bem como a duplicação dos esforços para desenvolver e aplicar essas tecnologias. Existe uma necessidade evidente e urgente de compartilhar boas práticas com base em evidências que comprovadamente impedem e reduzem as ocorrências.
- Atitudes sociais e outros fatores comportamentais que, em alguns países e culturas, facilitam que os agressores vitimizem crianças e adolescentes e não sejam detectados.
- A brecha digital geracional – com pais, responsáveis, educadores e políticos geralmente sem os recursos necessários para compreender a vida digital de crianças e adolescentes, ou para ajudá-los a entender e evitar os riscos *online*.
- Recursos insuficientes de forma geral, conscientização limitada e falha em desenvolver e compartilhar as melhores práticas sobre a proteção de crianças e adolescentes no ambiente *online*.

A ligação entre a segurança *online* de crianças e adolescentes e o desenvolvimento sustentável

Essas práticas não são apenas uma afronta aos direitos mais básicos de crianças e adolescentes, mas também ameaçam enfraquecer os possíveis benefícios que a transformação digital pode trazer a todos os países, principalmente para as sociedades em rápido desenvolvimento no Hemisfério Sul.

A União Internacional de Telecomunicações (UIT) estima que, para cada 10% de aumento na penetração dos serviços digitais, um país pode esperar 1,3% de crescimento do PIB *per capita* [8]. Porém, tais benefícios

Sobre o relatório

Este relatório foi elaborado pelo Grupo de Trabalho sobre Segurança *Online* de Crianças e Adolescentes da Comissão de Banda Larga. Esse GT multissetorial visa a tratar da segurança de crianças e adolescentes no ambiente *online* como um problema global. Ele foi formado por representantes sêniores de órgãos internacionais, incluindo agências da ONU, organizações não governamentais (ONGs), órgãos judiciais, reguladores e empresas privadas. Para a lista completa dos membros, consulte a página 3.

somente se materializam se todos os cidadãos, incluindo crianças e adolescentes, forem capazes de usufruir o máximo de benefícios possíveis a partir das oportunidades oferecidas pela conectividade. E isso somente pode acontecer se eles estiverem seguros quando no ambiente *online*.

Por essas razões, os Objetivos de Desenvolvimento Sustentável (ODS) da ONU também definem uma meta, no item 16.2, de acabar com o abuso, a exploração, o tráfico, a tortura e todas as formas de violência contra crianças e adolescentes até 2030. A fim de tomar as ações necessárias para conseguirmos cumprir essa meta ambiciosa, o Grupo de Trabalho elaborou a Declaração Universal de Segurança *Online* de Crianças e Adolescentes (*Child Online Safety Universal Declaration*).

A Declaração define os passos que as entidades públicas e privadas devem seguir para proteger crianças e adolescentes no ambiente *online*. Pedimos que todos os Estados assim como entidades privadas relevantes assinem a Declaração e se comprometam a colocar os seus princípios em ação.

Para ler e assinar a Declaração completa, acesse:

www.childonlinesafety.org

Introdução

3

Por que devemos tomar medidas agora para proteger crianças e adolescentes no ambiente *online*

A Comissão de Banda Larga para o Desenvolvimento Sustentável trabalha com os Estados-membros da ONU e com outros órgãos relevantes para promover a expansão da disponibilidade da internet de banda larga, principalmente em áreas nas quais as pessoas ainda não são atendidas de forma adequada.

Reconhecendo o papel transformador da conectividade, a Comissão decidiu priorizar a demanda pela conectividade em massa, uma vez que todas as evidências disponíveis demonstraram que estar conectado fomenta as oportunidades e o crescimento econômico.

A Comissão definiu metas para assegurar que, até 2025:

- 75% da população mundial estará *online*.
- 60% de todas as crianças e todos os adolescentes terão proficiência digital básica.
- 40% da população mundial utilizará serviços financeiros digitais.
- Mulheres e meninas terão igual acesso aos benefícios da conectividade.

Para atingir essas metas e perceber os benefícios que elas possibilitarão, é essencial que as ferramentas e os serviços digitais estejam acessíveis a todos em condições de igualdade. Isso não ocorre se grupos vulneráveis forem deixados sem a proteção adequada. E as crianças e os adolescentes são, de longe, a maior parcela demográfica vulnerável.

Uma pesquisa recente da UIT e da UNESCO identificou que, atualmente, mais de 50% da população mundial está *online* [9]. As crianças e os adolescentes constituem mais de 30% dos usuários da internet. Até 2022, mais 1,2 bilhão de novos usuários serão somados a essa quantidade, com crianças e adolescentes sendo o grupo demográfico *online* de mais rápido crescimento [10]. Até mesmo os países menos desenvolvidos do mundo estão no caminho de ter nos próximos anos a cobertura universal de internet móvel [11].

Essa explosão na conectividade beneficiará toda a humanidade, em particular os países de renda baixa e média nos quais há uma demanda enorme e não atendida da população por oportunidades econômicas, culturais e educacionais que o acesso à internet pode proporcionar.

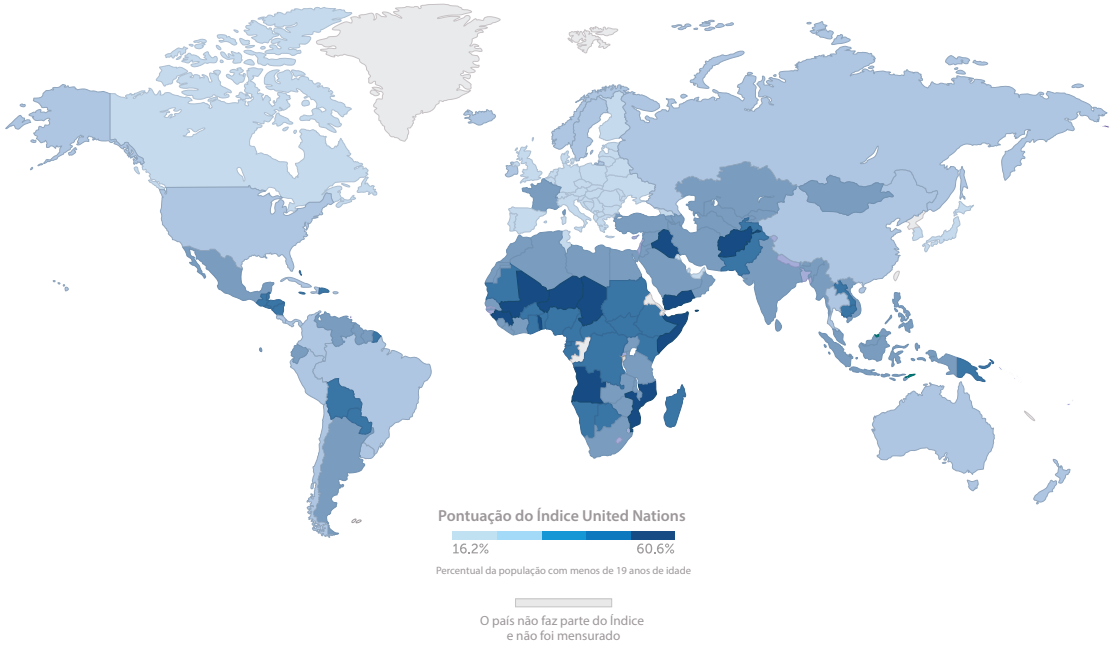
Desde 2011, 1,2 bilhão de pessoas abriram sua primeira conta bancária. Isso possibilitou que elas participassem de forma mais plena nos mercados locais e internacionais. E isso foi conquistado, em grande, parte graças ao aumento da inclusão digital e pelos bancos *online*, principalmente por meio dos telefones celulares [12].

Uma pesquisa da UIT mostra que o aumento da taxa de penetração dos serviços digitais estimula o crescimento econômico dos países [8]. O acesso confiável à internet também aumenta em até 13% as chances de uma pessoa obter emprego [8]. E isso está correlacionado a um aumento de 2,3% nos salários [8].

Nós não podemos considerar esses resultados positivos como garantidos. Em todo o mundo, há mais de 1 bilhão de crianças e adolescentes com menos de 18 anos [1]. Em alguns países em desenvolvimento, crianças e adolescentes compõem quase 50% da população [13]. Para entender o potencial total da transformação digital em âmbito global, essas crianças e esses adolescentes devem ser capazes de acessar, de forma segura, todas as oportunidades que a internet pode oferecer.

Infelizmente, pela experiência nos mercados desenvolvidos, nós sabemos que, sem que as proteções apropriadas estejam em vigor, a internet pode ser um ambiente difícil e – para alguns – perigoso para se crescer.

Onde vivem as crianças e adolescentes?



Fonte: United Nations, Department of Economic and Social Affairs, Population Division (2019). World Population Prospects 2019. Edição Online.

A maioria das crianças e dos adolescentes do mundo vive no Hemisfério Sul, em especial no continente africano, em nações que ainda estão no processo de digitalização.

> Nas palavras de uma jovem, quando pesquisadores lhe pediram para explicar por que crianças e adolescentes precisam ser ouvidos sobre a questão da segurança na internet: "É importante para os jovens poderem opinar sobre essas coisas, pois muitos adultos tentam pensar sobre como seria para um jovem na internet, mas eles não percebem o quanto os jovens são vulneráveis. Assim, é importante que os jovens tenham a chance de falar por eles mesmos" [14].

Crianças e adolescentes enfrentam diversos perigos e riscos *online*, desde serviços mal desenvolvidos que os vinculam – intencionalmente ou não – a contratos inadequados para a sua idade, por meio do *bullying* cibernético, da exposição a conteúdos inadequados, do assédio grave, do aliciamento *online*, do recrutamento por movimentos extremistas e da exploração e abuso sexual. É responsabilidade do mundo adulto encontrar uma forma de minimizar e impedir esses riscos e perigos.

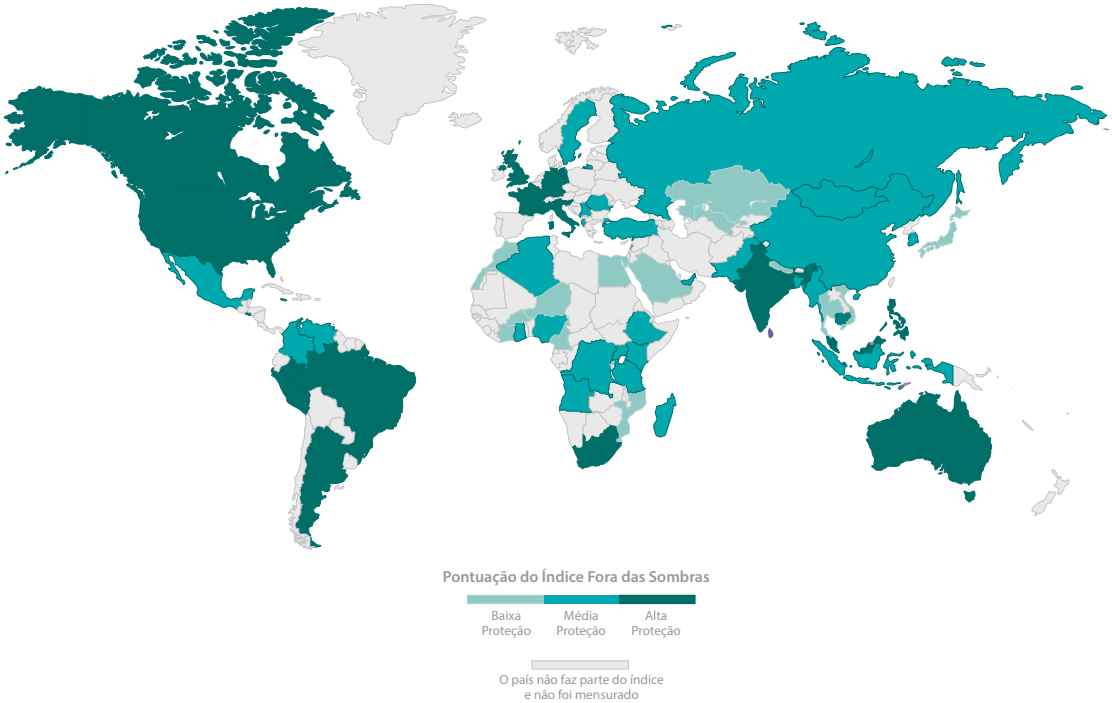
Com base nos achados da última pesquisa, este relatório resume a ampla variedade de riscos que crianças e adolescentes enfrentam no ambiente *online*.

Ele proporciona uma noção da escala e da natureza desses riscos e recomenda práticas e medidas concretas que vários atores podem tomar para minimizar os riscos, as ameaças e os perigos, bem como para deixar crianças e adolescentes mais seguros no ambiente digital.

Exemplos da escala e do alcance do problema

- Em apenas um ano, a *Internet Watch Foundation* (IWF) identificou mais de 105 mil *sites* que abrigam material de abuso sexual de crianças e adolescentes [15].
- Em 2018, a INHOPE confirmou a existência de 223.999 imagens e vídeos *online* que representavam atividades de exploração e abuso sexual de crianças e adolescentes.
- Um estudo de 2018 identificou que a maioria dos aplicativos móveis destinados a crianças e adolescentes coletava dados de maneiras que infringiam as normas de proteção de dados – e 19% deles coletavam informações de identificação pessoal [16].
- Estima-se que mais de 30% dos estudantes do ensino médio passarão por uma situação de *bullying* cibernético [17].

Existência de legislação de proteção contra o aliciamento *online*



Fonte: Out of the shadows: shining light on the response to child sexual abuse and exploitation. The Economist Intelligence Unit. 2019.

Dos 60 países incluídos no Índice Fora das Sombras (Out of the Shadows Index) da The Economist Intelligence Unit, apenas 21 apresentam legislação específica para proibir o aliciamento (grooming) de crianças e adolescentes no ambiente online (Fonte: EIU. Out of the shadows: shining light on the response to child sexual abuse and exploitation. The Economist Intelligence Unit, 2019. Disponível em: <https://outoftheshadows.eiu.com/>).

Em todos os lugares onde podemos coletar dados, nós vemos a mesma cena: muitas plataformas e serviços *online* não tomam as medidas adequadas para proteger crianças e adolescentes contra diversas violações. Como resultado disso, diversas crianças e adolescentes inevitavelmente se tornam vítimas deles.

Aprendemos com os países que já digitalizaram suas economias e sua infraestrutura social que existem medidas concretas que podem ser tomadas para tornar crianças e adolescentes mais seguros no ambiente *online*.

Isso inclui medidas como:

1. Criar o cargo de autoridade responsável no país pela segurança *online* de crianças e adolescentes.

2. Assegurar que uma legislação robusta esteja em vigor.

3. Assegurar que produtos e serviços sejam seguros por padrão e desde o seu *design*.

4. Criar um ecossistema conectado, no qual a prevenção, a detecção e a intervenção atuem continuamente e em conjunto.

5. Assegurar a coordenação com diferentes agências nos âmbitos nacional e regional, como entidades governamentais, setor privado, sociedade civil e instituições de pesquisa.

6. Educar crianças e adolescentes, pais e responsáveis sobre seus direitos, e assegurar que todos saibam para quem pedir ajuda se precisarem.

As medidas também incluem ter estatísticas e informações confiáveis – consistentes através das fronteiras – sobre as experiências de crianças e adolescentes no ambiente *online*.

Atualmente, muitas agências coletam dados estatísticos das faixas etárias de 0 a 14 e de 15 a 24 anos. Isso torna crianças e adolescentes invisíveis. Todos os dados devem tratar crianças e adolescentes com menos de 18 anos como um grupo distinto, para que as agências responsáveis por seu bem-estar tenham informações precisas, detalhadas e específicas para fundamentar suas estratégias e ações.

Também faltam definições comuns acordadas – por exemplo, para identificar quem é criança/adolescente ou o que constitui exploração e abuso sexual –, o que dificulta a construção de um panorama detalhado da situação da segurança *online* de crianças e adolescentes em todo o mundo.

É para tratar dessas falhas que o GT desenvolveu este relatório, com o intuito de priorizar a segurança *online* de crianças e adolescentes. A meta do GT é proporcionar aos leitores – principalmente membros dos governos, empresas do setor privado, incluindo prestadores de serviço de internet, membros da sociedade civil, ONGs e acadêmicos – um ponto de referência único, contendo informações sobre melhores práticas, respostas de políticas e ferramentas tecnológicas para serem usadas na luta contra o a exploração e o abuso sexual *online* de crianças e adolescentes.

Embora já existam excelentes estudos e relatórios sobre a segurança *online* de crianças e adolescentes – muitos deles realizados pelos membros especialistas do GT –, em geral esses relatórios enfocam um único problema ou forma de violência, tipicamente a exploração e o abuso sexual *online*. Porém, esse é apenas um aspecto do ambiente de ameaças *online*. Há vários outros problemas, como o *bullying*, jogos e a radicalização de crianças e adolescentes, entre muitos outros, que devemos tratar de forma coletiva para que meninas e meninos aproveitem todas as vantagens das oportunidades oferecidas a eles pelo advento da banda larga rápida e acessível.

O GT reconhece que a maior parte do conhecimento e das ferramentas de que os países e as empresas precisam para enfrentar esses problemas já existem (para obter mais detalhes, veja a seção "Recursos" no final deste relatório). Entretanto, existem desafios técnicos para a detecção e a execução, sendo muitos deles causados pelo crescimento da prática de criptografia dos conteúdos *online*. Porém, um desafio ainda maior é a falta de conscientização entre os principais interessados e tomadores de decisão quanto ao escopo e à magnitude dos riscos de segurança *online* de crianças e adolescentes, bem como das ferramentas já disponíveis para enfrentar esses riscos.

Desde 2010, a Iniciativa de Segurança *Online* de Crianças e Adolescentes (*Child*

Online Protection – COP) aborda esses problemas, ao fornecer uma plataforma para o compartilhamento de informações e para o aumento da conscientização. As Diretrizes de COP, da UIT, abordam amplamente o tema da proteção *online*, incentivando os *stakeholders* a tomar medidas para assegurar a proteção de meninas e meninos no ambiente digital.

Um obstáculo adicional para a priorização da segurança e do bem-estar de crianças e adolescentes é o estigma associado à discussão desses riscos, especialmente sobre o abuso sexual. Precisamos facilitar o acesso ao conhecimento, às ferramentas e fornecer àqueles que desejam ser agentes de mudança positiva os dados e informações de que precisam para mobilizar o compromisso de realizar investimentos na segurança *online* de crianças e adolescentes.

Neste relatório, enfocamos a situação atual de crianças e adolescentes *online*. Que oportunidades estão surgindo para eles? Quais riscos e perigos eles enfrentam? Como os riscos os impedem de ter acesso às oportunidades mencionadas? E o que podemos fazer para assegurar que isso não aconteça? Nosso principal objetivo consiste em refletir sobre como priorizar a segurança *online* de todas as crianças e todos os adolescentes, mas particularmente os dos países de baixa renda, onde frequentemente as estruturas de proteção na são suficientemente desenvolvidas, o que aumenta os riscos de violações.

Ao longo de todo o relatório, o GT fez o seu melhor para fornecer recursos e sugestões que serão adequados para diversos mercados, cada um com suas próprias combinações de tecnologias, pressões sociais e outros fatores de influência, reconhecendo ainda que uma medida única para todos não é a solução. Este relatório deve ter a mesma utilidade para os leitores de países de renda baixa e média com altos níveis de penetração de banda larga móvel, mas com poucas linhas de telefone fixo, como acontece em mercados mais consolidados.

Trabalhando em conjunto, através das fronteiras, acreditamos que podemos construir um ecossistema na internet que fomente a criatividade e aproveite a energia da próxima geração. Com a liberdade de explorar um mundo digital cada vez mais conectado, sem medo de qualquer perigo, crianças e adolescentes expandirão seus horizontes e estarão à altura do desafio de atingir seu potencial. Ao fazer isso, eles fortalecerão a próxima onda de crescimento econômico e de mudança social positiva.

Este relatório, que enfoca as crianças e os adolescentes, complementa o relatório elaborado pelo Painel de Alto Nível em Cooperação Digital da Secretaria-Geral da ONU, que coloca a segurança *online* de crianças e adolescentes em um contexto mais amplo de direitos digitais e de cooperação digital.

A Declaração Universal da Segurança *Online* de Crianças e Adolescentes ligada a este relatório é uma ferramenta para ajudar a mobilizar e ampliar os compromissos dos governos, do setor privado e da sociedade civil para priorizar a proteção *online* de crianças e adolescentes, por meio de uma estrutura comum e de ações concretas.

O que são crianças e adolescentes?

Ao longo deste relatório, define-se criança e adolescente como qualquer pessoa com menos de 18 anos de idade. Isso está de acordo com o Artigo 1º da Convenção sobre os Direitos da Criança da ONU (*UN Convention on the Rights of the Child* – UNCRC). Na prática, alguns mercados tratam como adulto qualquer indivíduo que tenha idade suficiente para consentir quanto ao processamento de dados, o que pode significar alguém com apenas 13 anos de idade. Esse conflito não é justificado por qualquer evidência nos marcos legais de desenvolvimento infantojuvenil. Por outro lado, ele enfraquece os direitos e ameaça a segurança de crianças e adolescentes. Veja na página 76 um estudo de caso que traça o impacto da UNCRC nos direitos de crianças e adolescentes em todo o mundo.

Como seria um ambiente mais seguro?

4

Como seria um ambiente mais seguro?

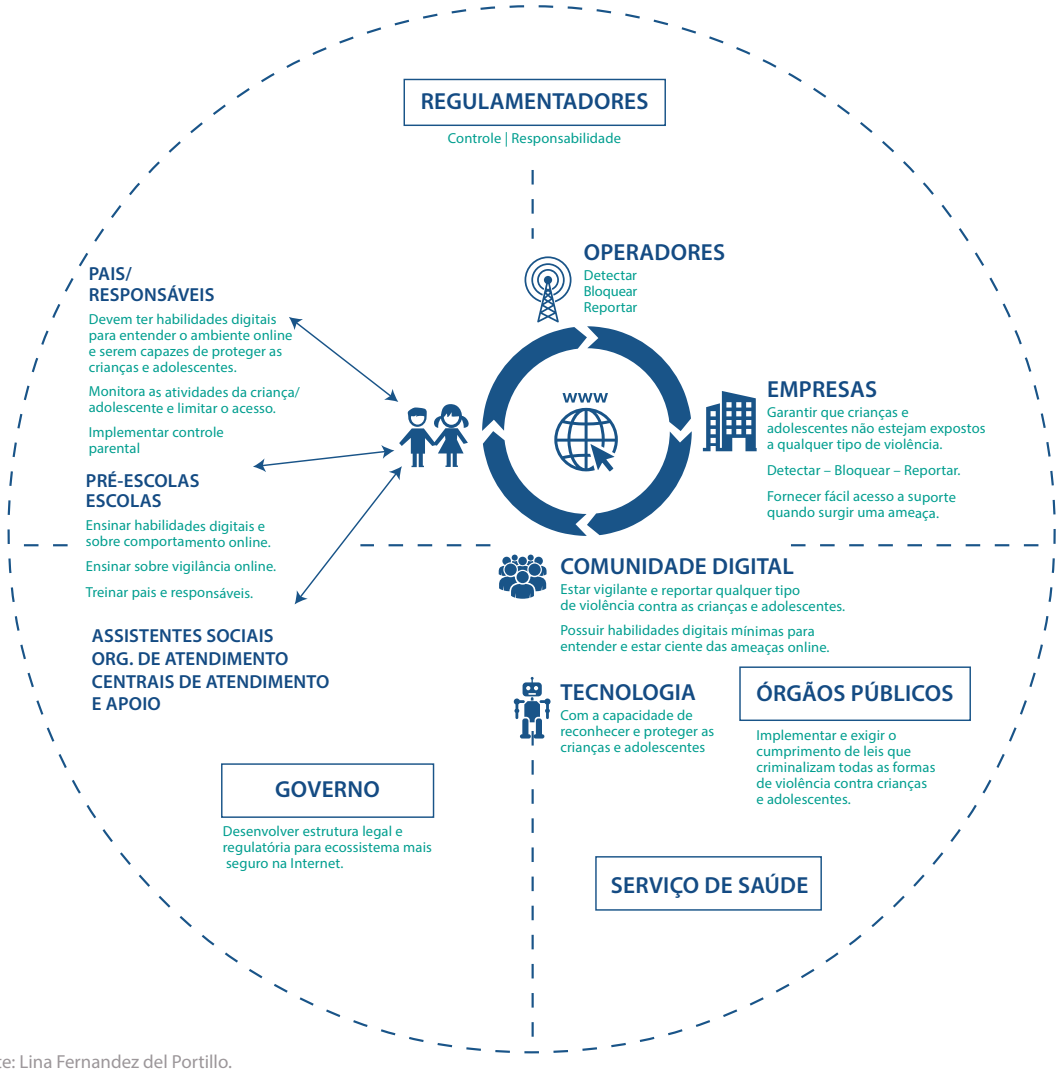
Milhões de crianças e adolescentes em países de renda baixa e média, ainda no processo de digitalização, geralmente não estão protegidos de forma adequada no ambiente *online*. Precisamos resolver isso com urgência, para manter crianças e adolescentes seguros e assegurar que obtenham o maior benefício possível no ambiente digital.

Isso é particularmente importante nos países em desenvolvimento, os quais detém o maior percentual de crianças e adolescentes.

Esses países devem se beneficiar mais com a conectividade, de modo a obter acesso à educação de qualidade, ao entretenimento, à saúde e a outros serviços.

Para entendermos o que deve ser feito para manter crianças e adolescentes mais seguros quando se conectam no ambiente *online*, devemos primeiro

Ecossistema da internet mais segura



Fonte: Lina Fernandez del Portillo.

Para proteger integralmente crianças e adolescentes dos perigos ou da exposição desnecessária a riscos online, todos os stakeholders relevantes devem estar bem informados, empoderados e engajados.

entender o que significa "mais seguro". Como seria um sistema no qual crianças e adolescentes estariam tão seguros quanto os adultos? E como uma criança ou adolescente vivenciaria a internet dentro desse sistema?

Crianças ou adolescentes mais seguros estão protegidos por uma base legal mais robusta

Para proteger crianças e adolescentes contra a violência sexual *online*, um país deve ter uma base legal robusta que defina os direitos de crianças e adolescentes, os crimes cometidos contra eles e as penas que os criminosos receberão. Um bom ponto de partida é incorporar às leis nacionais as convenções internacionais relevantes.

Essas convenções e protocolos internacionais são:

- **A Convenção sobre os Direitos da Criança da ONU (UNCRC, 1989)**: consagra diversos direitos de crianças e adolescentes, incluindo direitos civis, culturais, econômicos, políticos e sociais.
- **Protocolo Facultativo à Convenção sobre os Direitos da Criança referente à venda de crianças, à Prostituição Infantil e à Pornografia Infantil (2002)**: uma base para analisar as abordagens aos crimes que envolvem materiais sobre abuso sexual de crianças e adolescentes.
- **Convenção de Budapeste sobre Crimes Cibernéticos (2001) –** o primeiro instrumento intergovernamental obrigatório que trata dos crimes de pornografia de crianças e adolescentes facilitados por computadores.
- **O Conselho da Convenção Europeia sobre Proteção de Crianças e Adolescentes contra Exploração e Abuso Sexual (2007) –** trata dos crimes que envolvem materiais sobre abuso sexual de crianças e adolescentes e dos crimes de aliciamento de menores *online* (*grooming*).

A adoção da Agenda de Desenvolvimento da ONU pós-2015 com os 17 ODS pela Assembleia Geral das Nações Unidas (ONU) apresenta novas oportunidades para priorizar a proteção *online* de crianças e adolescentes. Uma criança ou um adolescente que utiliza a internet em um território que incorpora essas medidas e que aderiu aos ODS deve contar com diversos direitos previstos.

Esses direitos devem moldar o ambiente legal e regulatório dos prestadores de serviço da internet e das empresas de tecnologia que fornecem acesso à internet. Também impõem obrigações e orientam as ações das agências responsáveis pelo bem-estar de crianças e adolescentes.

Para mais informações, consulte a página 66, para obter um modelo das medidas voltadas à proteção *online* de crianças e adolescentes, com o intuito de ser um exemplo para os países utilizarem quando da atualização dos seus planos nacionais de banda larga.

Para ler sobre iniciativas de sucesso realizadas por órgãos legais e seus parceiros na Albânia e nas Filipinas, veja os estudos de caso nas páginas 77 e 78.

Uma cultura empresarial que promove ativamente a segurança de crianças e adolescentes

Para que crianças e adolescentes tenham o maior grau possível de segurança no ambiente *online*, eles devem poder contar com as empresas que prestam os serviços necessários para praticar a proteção ativa de crianças e adolescentes. Em suas Diretrizes para a Indústria sobre Proteção *Online* de Crianças e Adolescentes (Iniciativa COP), de 2015, o UNICEF identifica cinco regras que as empresas de tecnologia devem

obedecer para proteger crianças e adolescentes que utilizam seus produtos e serviços:

1. Os direitos de crianças e adolescentes devem estar integrados em todas as políticas e em todos os processos apropriados da empresa.

2. A empresa deve ter processos estabelecidos para lidar com a violação dos direitos de crianças e adolescentes.

3. Os ambientes oferecidos pelas empresas devem ser apropriados para a idade dos usuários.

4. A empresa deve educar crianças e adolescentes, seus pais e responsáveis sobre como utilizar seus produtos de forma responsável.

5. A tecnologia digital deve ser promovida como uma forma de aumentar o engajamento cívico.

Para mais detalhes, leia as Diretrizes para a Indústria sobre Proteção Online de Crianças e Adolescentes do UNICEF (em inglês): https://www.unicef.org/csr/files/COP_Guidelines_English.pdf

Para estarem mais seguros, crianças e adolescentes devem conhecer os seus direitos

Crianças e adolescentes devem conhecer e entender os seus direitos o mais cedo possível. Isso capacita a criança ou a adolescente a reconhecer quando algo está errado para, assim, alertar um adulto responsável e ser capaz de denunciar uma violação a seus direitos. Para isso acontecer, professores e pais também devem entender os direitos de crianças e adolescentes no ambiente *online* e ser capazes de transmitir essa informação, em uma linguagem que seja apropriada para a idade de cada criança ou adolescente [18].

O papel crucial da educação

Para proteger crianças e adolescentes, os professores, os pais e os responsáveis devem ter, no mínimo, habilidades digitais básicas: o suficiente para ajudar as crianças e os adolescentes a obterem o máximo de benefício do fato de estarem conectados, ao mesmo tempo em que reconhecem e respondem apropriadamente aos perigos em potencial. Porém, em mercados que experimentam uma rápida transformação digital, os adultos geralmente não possuem o conhecimento para ajudar as crianças e os adolescentes.

O Instituto DQ, um centro de pesquisa internacional dedicado a estabelecer padrões globais de inteligência digital para a educação, definiu oito áreas-chave de habilidades digitais que uma criança ou um adolescente deve dominar para estar seguro e ter uma experiência positiva no ambiente *online*.

Essas oito áreas são:

- **Identidade digital –** a capacidade de criar e manter uma identidade positiva *online*.

- **Uso digital –** a capacidade de utilizar a tecnologia de uma forma saudável e equilibrada.

- **Proteção digital –** a capacidade de minimizar diversos riscos *online*.

- **Segurança digital –** a capacidade de administrar e evitar riscos aos dispositivos e dados.

- **Inteligência emocional digital –** a capacidade de reconhecer, navegar e expressar emoções no ambiente *online*.

- **Comunicação digital –** a capacidade de comunicar e colaborar utilizando a tecnologia.

- **Alfabetização digital –** a capacidade de encontrar, ler, avaliar, criar e compartilhar informações no ambiente digital.

- **Direitos digitais –** a capacidade de entender e sustentar os direitos humanos e legais no ambiente *online*.

Todas essas oito competências são importantes para que uma criança ou adolescente tenha total acesso a seus direitos *online*. Nos estudos, essa abordagem demonstrou ser satisfatória. Crianças e adolescentes treinados nas oito competências apresentarem 15% menos risco de sofrer algum tipo de perigo *online* em relação aos que que não foram treinados [19].

No contexto atual, pesquisas do UNICEF identificaram que 43% de crianças e adolescentes da África do Sul dizem que nunca ou raramente pedem orientação aos pais sobre as coisas que acontecem no ambiente *online* [20]. Esses números foram bastante similares entre os mercados estudados: na Itália, por exemplo, a proporção foi 53% [21] e, na Sérvia, 46% [22].

Apenas a educação – fornecendo habilidades digitais, incluindo o direito de crianças e adolescentes de estarem seguros no ambiente *online* e o que todos os *stakeholders* podem fazer para assegurar esse direito – pode suprir essa falha. E a forma mais fácil de proporcionar essa educação é por meio de professores, pais e responsáveis. É por isso que fornecer habilidades digitais a todas as crianças e a todos os adolescentes deve ser um direito universal.

Professores, pais e responsáveis têm o papel-chave de assegurar que crianças e adolescentes saibam como utilizar a tecnologia digital de forma responsável e segura. Reuniões e seminários conjuntos para educadores, estudantes, pais e responsáveis podem ajudar a sensibilizar as crianças e os adolescentes sobre os perigos que o comportamento de risco no ambiente *online* podem causar.

Como garantir a segurança de crianças e adolescentes desde o *design* do produto

Para estar o mais segura possível, uma criança ou um adolescente deve ter à disposição *softwares*, aplicativos e sistemas que sejam apropriados para sua idade, e que foram criados especificamente para crianças e adolescentes. Os *softwares* ou serviços produzidos para serem seguros desde sua origem e apropriados para a idade devem:

- Assegurar o melhor interesse da criança ou do adolescente como o principal princípio do seu *design*.

- Ser apropriado para a idade, com uma robusta função de verificação de idade.

- Ser transparente e responsável sobre como utiliza e coleta os dados pessoais.

- Coletar e reter apenas os dados que necessitam para cumprir sua função.

- Apresentar políticas e padrões de comportamento que protegem crianças e adolescentes contra vários perigos.

- Instalar em suas configurações um padrão que prioriza a privacidade acima de qualquer outra consideração.

- Compartilhar dados apenas em casos de extrema necessidade e considerando o melhor interesse da criança ou do adolescente.

- Incluir o *feedback* e a comunicação com crianças e adolescentes, pais ou responsáveis sobre conteúdos ou comportamentos inadequados.

Leitura adicional

Os reguladores do Reino Unido e da Austrália elaboraram guias claros e abrangentes para criar sistemas que sejam seguros para crianças e adolescentes desde o *design* dos produtos e serviços.

No Reino Unido, o responsável pela área de Informações irá introduzir em breve o Código do Desenvolvimento Apropriado para a Idade (*Age Appropriate Design Code*), um código de prática obrigatório que define as proteções específicas que crianças e adolescentes devem ter para seus dados [24]. Ele oferecerá a todos os menores de 18 anos uma alta proteção de dados desde o *design*, como padrão e aplicável a todos os serviços que são "prováveis de serem acessados" por crianças e adolescentes.

Na Austrália, a Comissão de Segurança Eletrônica desenvolveu um conjunto de Princípios de Segurança por *Design* e iniciou o trabalho para criar um marco de orientação para o uso na indústria [25]. A Comissão está realizando uma consulta sobre as ferramentas e os recursos necessários para assegurar que a segurança de crianças e adolescentes seja integrada no *design* do serviço.

Mais informações podem ser encontradas em: ico.org.uk e www.esafety.gov.au

Assegurar que os *softwares*, os aplicativos *webs*, os *apps* e os *websites* sigam essas normas é uma das formas mais efetivas pelas quais o setor privado, principalmente as empresas de tecnologia, podem contribuir para proteger crianças e adolescentes no ambiente *online*.

Para ser seguro desde o *design*, a tecnologia deve ter proteções integradas contra os seguintes tipos de risco:

1. Riscos de contato – a criança ou o adolescente se envolve em uma comunicação que pode trazer algum perigo (isso inclui riscos como perseguição *online*: agressores que fingem ser crianças e adolescentes e que observam seus padrões de uso específicos para identificar vítimas solitárias ou em potencial).

2. Riscos de conteúdo – a criança ou o adolescente visualiza um conteúdo indesejado ou prejudicial.

3. Riscos de conduta – comportamento perigoso entre crianças e adolescentes, como, por exemplo, *bullying*, troca de mensagens de texto de conteúdo sexual (*sexting*) etc.

4. Riscos de contrato – serviços *online* devem assegurar que um adulto responsável tenha consentido para a participação da criança ou do adolescente.

Os perigos que se enquadram nessas categorias incluem exploração e abuso sexual, tráfico, recrutamento por movimentos radicais, conteúdo e atividades ilegais e inadequados para a idade, conteúdo que promove ferimentos ou automutilação, contatos pessoais que sejam ilegais ou perigosos (como o aliciamento de crianças e adolescentes), perseguição ou *bullying*. Essas atividades que não são apropriadas para a idade com frequência são permitidas tecnicamente pelo fato de os termos e condições do prestador *online* não terem sido elaborados considerando crianças e adolescentes.

O papel da tecnologia para tornar crianças e adolescentes "mais seguros" no ambiente *online*

A tecnologia por si só não tornará crianças e adolescentes mais seguros. Uma empresa ou serviço pode ter o *software* de proteção de crianças e adolescentes mais sofisticado disponível e, ainda assim, se sua segurança e seus direitos não forem fundamentais para a opinião pública, a educação, a política, o *design* do produto e as operações, crianças e adolescentes não estarão seguros.

Evidências recentes também indicam que os controles parentais podem não ser tão efetivos em prevenir os perigos como se acreditava anteriormente [27].

No contexto da cultura e da prevenção de crimes, a tecnologia tem um papel vital a desempenhar, uma vez que a maioria dos serviços conta com usuários demais para depender apenas do monitoramento humano. O sistema desempenha um papel crucial em impedir os perigos e sinalizar comportamentos graves para chamar a atenção dos moderadores humanos.

As tecnologias de proteção de crianças e adolescentes incluem:

- **Tecnologias de bloqueio –** geralmente operando no nível de prestadores de serviços de internet (ISPs), as tecnologias de bloqueio reconhecem e bloqueiam *sites* ou conteúdos que promovem perigos a crianças e adolescentes.

- **Filtro heurístico –** tecnologias que buscam variáveis como endereço IP, conteúdo, palavras-chave e bloqueiam *sites* que não estão na lista negra, mas que podem conter conteúdo prejudicial.

- **Detecção automática de materiais sobre abuso sexual –** utilizando soluções como classificadores, que tomam como referência listas negras de materiais sexuais que envolvem crianças e adolescentes, os prestadores podem instantaneamente indicar, bloquear e/ou relatar conteúdos de abuso sexual.

- ***Web crawlers* –** buscando as mesmas variáveis que os filtros (palavras-chave, materiais sexuais que envolvem crianças e adolescentes, imagens etc.), os *web crawlers* buscam ativamente *sites* prejudiciais e, então, alertam as autoridades.

- **Reconhecimento facial –** utilizando a tecnologia de reconhecimento facial, as autoridades e outros atores do setor podem identificar rapidamente vítimas e agressores conhecidos.

Muitas dessas tecnologias contam com a utilização da inteligência artificial (IA). Sem ela, não seria possível nem a proteção em escala em tempo real, nem a indicação de padrões com base em tendências de longo prazo, considerando o volume de dados gerados todos os dias no ambiente *online*.

Entretanto, é preciso ter cautela. Os principais estudiosos que trabalham com IA advertem que muitos algoritmos são tendenciosos. Por exemplo, como não controlam de forma suficiente a correlação *versus* a causalidade, com as informações que geram, eles podem induzir os usuários humanos a ver uma relação entre dois fenômenos que, na verdade, não existe [26].

Outro desafio relativo às soluções totalmente automatizadas é que alguns dos riscos que afetam crianças e adolescentes – o aliciamento de menores e o *bullying*, por exemplo – dependem do contexto, e esses sistemas não têm a capacidade de interpretar o contexto (humano).

Isso pode levar – entre outros aspectos – a resultados gerados por IA que discriminam minorias, mulheres, meninas e outros grupos tradicionalmente desfavorecidos. Considerando esses limites da tecnologia, a revisão e a intervenção

humana continuam sendo um elemento de importância essencial no espaço de proteção *online* de crianças e adolescentes. Neste momento, nenhuma ferramenta de IA de proteção de crianças e adolescentes deve ser usada sem proteções e protocolos adicionais para assegurar a precisão dos dados.

Outro desafio é que muitos sistemas digitais enfocam os adultos e precisam de decisões ou ações com pequenas nuances que não são apropriadas para crianças e adolescentes. Para solucionar esse problema, devemos assegurar que os sistemas forneçam a crianças e adolescentes proteções especiais, e que não esperem que estes sejam capazes de tomar decisões como adultos.

Um resumo do que significa estar "mais seguro"

Concluindo, uma criança ou um adolescente que está o mais seguro possível:

- Estará protegido por uma base legal robusta, efetiva e em vigor, que protege os direitos de crianças e adolescentes.
- Utilizará soluções e serviços apropriados para crianças e adolescentes, os quais foram desenvolvidos para protegê-los e minimizar os possíveis riscos.
- Estará empoderado por um conjunto de habilidades digitais abrangentes que permita que essa criança ou adolescente minimize os riscos *online* e maximize os potenciais que a internet oferece; reconheça quando seus direitos estão sendo violados; e possa ser apoiado ou apoiada por adultos que entendem seus direitos e saibam como protegê-los *online*, com acesso a mecanismos seguros e confiáveis para reportar quaisquer violações a esses direitos.

5

A situação atual de crianças e adolescentes no ambiente *online*

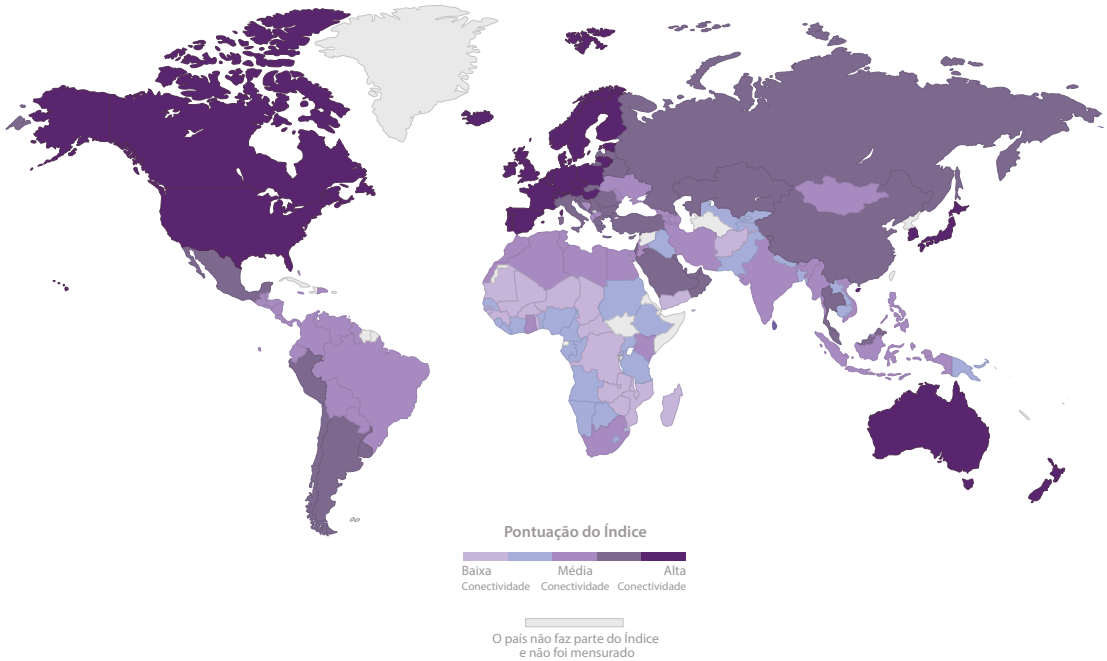
A situação atual de crianças e adolescentes no ambiente *online*

De acordo com a pesquisa do UNICEF, em todo o mundo, 71% de crianças e adolescentes já estão *online* [28]. A disponibilidade de *smartphones* com preço acessível e banda larga móvel está tornando ainda mais fácil que crianças e adolescentes estejam *online*. De acordo com a UIT, nos países menos desenvolvidos, 35% dos usuários da internet são jovens, enquanto 13% estão nos mercados mais consolidados digitalmente [29].

Contudo, ainda existem partes do mundo nas quais milhões de jovens ainda aguardam por sua primeira conexão. Na África, por exemplo, 60% dos jovens ainda não estão *online* [30]. Porém, com o número de usuários africanos da internet aumentando 20% ao ano [31], muitos desses jovens em breve estarão *online*. O mesmo acontece nos países menos desenvolvidos ao redor do mundo, onde 70% dos jovens ainda não estão *online* [29]. Ainda existe também uma enorme desigualdade de gênero nos países menos desenvolvidos: as meninas têm uma probabilidade 71% menor de ter acesso à internet [32].

Na África Subsaariana, na Ásia e na América Latina, a conectividade ainda não chegou a todas as crianças e adolescentes. Com a expansão da banda larga acessível a essas partes do mundo em desenvolvimento, há uma necessidade urgente de se implementar medidas para minimizar os riscos e as ameaças a esse público, ao mesmo tempo em que existe a necessidade de se permitir que eles tirem proveito de todos os benefícios que o mundo digital pode trazer para as nossas sociedades.

Índice de Conectividade Móvel GSMA: Situação da conexão móvel ao redor do mundo em 2018

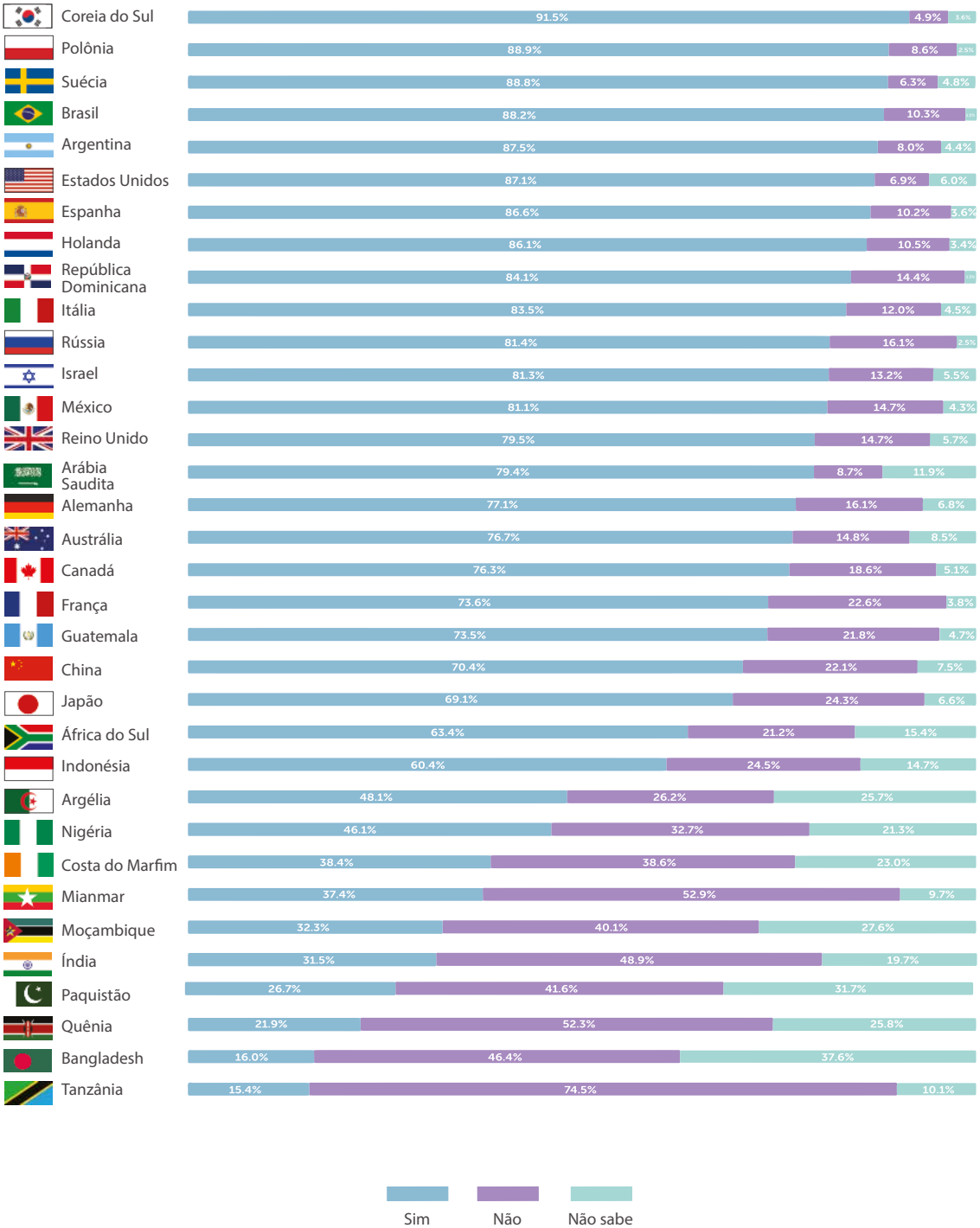


Fonte: GSMA Global connectivity Index 2019. GSMA Intelligence Unit
https://www.mobileconnectivityindex.com/#year=2018

Nas nações desenvolvidas, a conectividade móvel está se tornando onipresente. No futuro próximo, isso também ocorrerá em muitos países em desenvolvimento.

Uso do telefone celular para acessar a Internet por crianças e adolescentes em 34 países.

Seu filho/algum de seus filhos (entre 5 e 17 anos) utilizou a internet em um telefone celular nos últimos 3 meses?



Fonte: GSMA Intelligence Unit

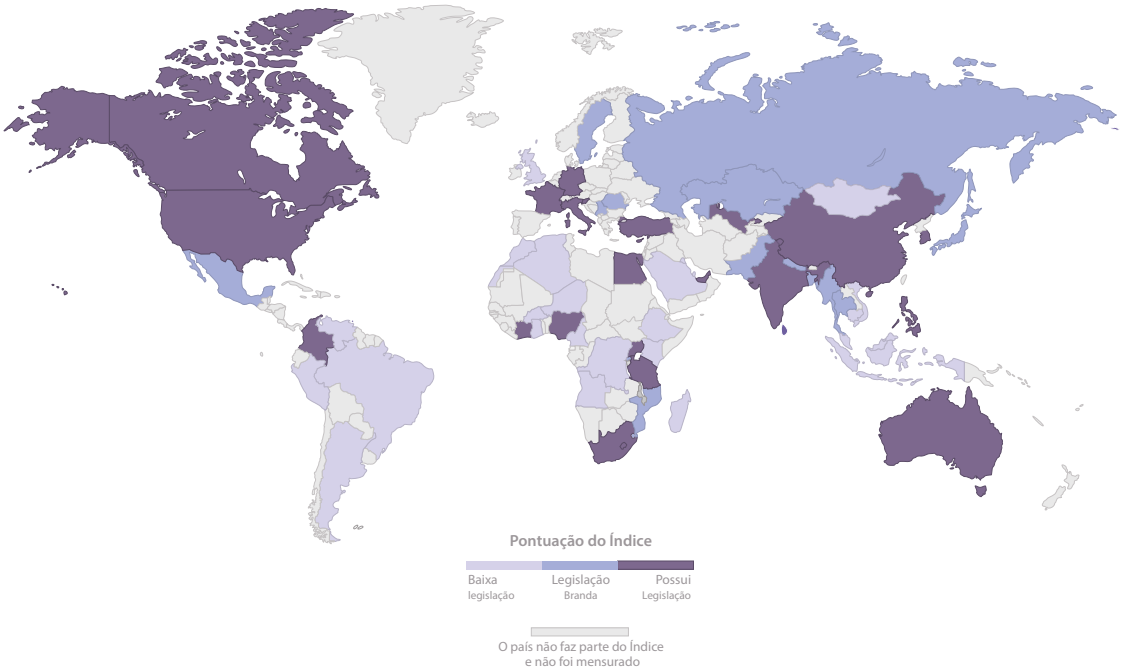
Pesquisas e estudos mostram que a maioria das crianças e dos adolescentes nos países desenvolvidos e em muitos países em desenvolvimento já usa regularmente telefones celulares para acessar a internet.

Por que devemos agir agora para proteger crianças e adolescentes

Nenhum país possui sistemas de proteção *online* de crianças e adolescentes perfeitos em vigor. Mesmo nos países de alta renda, com o histórico de duas décadas de crescimento da internet, geralmente ainda existem falhas no ecossistema de proteção *online* de crianças e adolescentes.

Se um foco global renovado na segurança digital de crianças e adolescentes incentivasse os reguladores e legisladores a suprir essas falhas, as ramificações positivas para crianças e adolescentes seriam profundas. Em diversos países, estão sendo feitas perguntas de pesquisa sobre se ainda é o melhor modelo confiar nos mecanismos auto regulatórios para realizar mudanças progressivas quanto a crianças e adolescentes. As dúvidas

Proteção na Internet por uma perspectiva legislativa
Reporte obrigatório, bloqueio de conteúdo, detecção e manutenção de registro de materiais sexuais envolvendo crianças e adolescentes



Fonte: Out of the shadows: shining light on the response to child sexual abuse and exploitation. The Economist Intelligence Unit. 2019.

Nesse caso, o Índice Fora das Sombras (Out of the Shadows Index) identificou que apenas 9 entre 60 países estabeleceram em sua legislação relatos obrigatórios, bloqueio de conteúdo, exclusão e registro de materiais sobre abuso sexual de crianças e adolescentes. Para enfatizar essa pequena lista, temos a África do Sul, a China, as Filipinas, a Índia, a Tanzânia e a Turquia. Das três ações esperadas, 11 países realizam apenas duas, e 15, apenas uma. Além disso, 25 dos 60 países não fazem nada sobre essa questão específica.

atuais sobre o impacto da criptografia de ponta a ponta nos esforços globais para identificar e acabar com a distribuição de materiais sexuais que envolvem crianças e adolescentes demonstram a urgência dessas questões [33] [34].

Em alguns países que atualmente passam pela digitalização, não existem leis, políticas, sistemas, nem tecnologias necessárias para manter crianças e adolescentes seguros. Exceto por alguns exemplos, como Ruanda (ver Estudo de Caso 2, na página 77), o impulso para expandir a conectividade não foi acompanhada pelo mesmo nível de esforço para assegurar a segurança de crianças e adolescentes. Isso não apenas

expõe milhões de crianças e adolescentes a perigos, mas também arrisca reduzir a capacidade da transformação digital de proporcionar o progresso econômico e social.

O alcance dos materiais sobre abuso sexual de crianças e adolescentes no ambiente *online*

De acordo com o trabalho realizado pela OMS, todos os anos, 200 milhões de crianças e adolescentes sofrem violência sexual [7]. E, cada vez mais, a maior parte desses casos de violência sexual ocorre no ambiente *online* ou é obtida e distribuída digitalmente. Nesse caso, a internet é uma facilitadora da exploração e do abuso sexual.

O banco de dados de Exploração Sexual de Crianças e Adolescentes da Interpol tem mais de 1,5 milhão de imagens e vídeos, registrando coletivamente a violência sexual de mais de 19,4 mil vítimas em todo o mundo [35]. Nos EUA, o Centro Nacional de Crianças e Adolescentes Perdidos e Explorados (NCMEC) tem um banco de dados de mais de 25 milhões de arquivos contendo imagens de crianças e adolescentes [36]. Reconhece-se que esses números são apenas uma pequena fração de todos os materiais sexuais disponíveis que envolvem crianças e adolescentes (fotos únicas e cópias das cópias), e que muitos continuam não detectados. É alarmante que o número de relatos da Cyber Tipline recebido pelo NCMEC tenha aumentado quase dez vezes em três anos, de 1,1 milhão em 2014, para 10,2 milhões em 2017, e quase dobrou em 2018, com 18,4 milhões de relatos recebidos.

A Associação Internacional de Canais de Denúncia (INHOPE), atua com 46 canais de denúncias participantes em 41 países. Quando alguém denuncia um material sexual envolvendo crianças e adolescentes que é abrigado em um país que não aquele onde o canal de denúncia está localizado, a INHOPE informa o canal de denúncia do país de abrigo em questão, utilizando sua solução segura de *software*, ICCAM, financiada pela Comissão Europeia [107].

A "Pesquisa internacional de sobreviventes" realizada pelo Centro Canadense de Proteção à Criança também mostra que as crianças mais jovens estão em situação de maior risco, com 56% das vítimas indicando que o abuso sexual que sofreram começou antes dos 4 anos de idade, e 87% com menos de 11 anos [38].

Em 2018, a *Internet Watch Foundation* (IWF) anunciou um aumento de 32% no número de *sites* denunciados que continham materiais sexuais envolvendo crianças e adolescentes [37]. Foram encontrados os seguintes dados quanto ao conteúdo de materiais sobre abuso sexual de crianças e adolescentes:

- 39% das vítimas tinham menos de 10 anos, 55% tinham entre 11 e 13 anos, e 5% tinham entre 14 e 15 anos.
- 78% dos materiais sexuais envolvendo crianças e adolescentes retratavam meninas, 17% retratavam meninos e 4% retratavam ambos os sexos.
- 23% de todos os materiais sexuais envolvendo crianças e adolescentes *online* em 2018 eram do tipo mais grave, incluindo imagens de estupro e tortura.
- 82% dos materiais sobre abuso sexual de crianças e adolescentes foram encontrados em *sites* que abrigam imagens sem verificação do usuário, ou com verificação limitada.

O desafio do conteúdo gerado automaticamente

Apenas nos seis primeiros meses de 2019, a IWF recebeu 22.482 relatos de materiais sexuais autogerados envolvendo crianças e adolescentes: um terço de todos os relatos aos quais a IWF respondeu. Das vítimas retratadas nesse conteúdo, 96% eram meninas, e 85% tinham entre 11 e 13 anos. Essas imagens e esses vídeos mostram crianças e adolescentes, geralmente em um contexto doméstico, que foram aliciados ou coagidos a realizar atos sexuais para espectadores por meio de uma *webcam*. Os agressores registraram as imagens e as compartilharam *online*.

A pesquisa realizada pelo *End Child Prostitution and Trafficking* (ECPAT) identificou que 56% das vítimas nos materiais sexuais envolvendo crianças e adolescentes eram pré-adolescentes, e que 4,3% eram bebês ou crianças pequenas.

Além disso, quanto mais jovem era a vítima, maior era a probabilidade de o abuso ser grave [39].

De acordo com um relatório realizado pela NetClean, que é especializada em soluções que identificam materiais sexuais envolvendo crianças e adolescentes *online*, 85% dos policiais que investigam a violência sexual contra crianças e adolescentes no ambiente *online* dizem ter encontrado grupos organizados de agressores em fóruns e comunidades *online*.

Além disso, quase metade dos policiais pesquisados relataram que o número de grupos organizados estava crescendo [40].

Riscos de contato: aliciamento, *bullying* cibernético, *stalking* e assédio

O *bullying* cibernético é outra violação aos direitos de crianças e adolescentes. O UNICEF define o *bullying* cibernético como o uso de mensagens eletrônicas para assediar, ameaçar ou atacar outra pessoa. Com frequência, os adultos não estão cientes de que isso está acontecendo, então não podem ajudar. Por conta da conectividade, ambientes que um dia já foram seguros para crianças e adolescentes, em especial suas casas, se transformam em uma arena secreta de tormentos. Curiosamente, um estudo de 2018 identificou que os adolescentes frequentemente consideram o *bullying* cibernético como algo normal e não querem envolver seus pais – o que aumenta seu isolamento [41].

Ao mesmo tempo, uma pesquisa realizada em 28 países, incluindo Brasil, China, Estados Unidos, Índia e Rússia, identificou que, em média, 17% dos pais disseram que seus filhos já haviam sido vítimas de *bullying* cibernético. Em alguns países, esse número chegou a 37% [3].

Outro aspecto do *bullying* é o assédio sexual *online*. Um estudo de 2017 com crianças e adolescentes na Dinamarca, na Hungria e no Reino Unido identificou que 6% das deles haviam tido fotos explícitas compartilhadas sem a sua permissão. Ainda nessa amostra, 25% haviam sido objeto de boatos sobre sua vida sexual. E 31% haviam visto pessoas da mesma idade criarem perfis falsos para compartilhar fotos sexuais de um terceiro.

Ainda mais preocupante: 9% haviam recebido ameaças sexuais de pessoas da mesma idade [42].

Por fim, outra forma bem conhecida de contato de risco é o aliciamento (*grooming*). O Centro Internacional de Crianças e Adolescentes Desaparecidos e Explorados (*International Centre for Missing*

Recrutamento por movimentos radicais como aliciamento

Em 2014, três meninas norte-americanas, estudantes do ensino médio na cidade de Denver, foram interceptadas na Alemanha no caminho para se juntarem ao grupo *jihadista* do Estado Islâmico (EI) [45].

As três haviam sido recrutadas no ambiente *online*. A maioria dos países do Ocidente e do Oriente Médio testemunhou casos similares. Esse também não é um problema relacionado exclusivamente ao EI. Em todo o mundo, existem inúmeros grupos e movimentos extremistas – incluindo o Talibã, o Al Shabab e grupos de supremacia branca, entre outros – que buscam recrutar crianças e adolescentes. Nesses cenários, crianças e adolescentes estão extremamente vulneráveis e, uma vez nas mãos de seus aliciadores, podem achar que é impossível escapar. Por esse motivo é tão importante desenvolver sistemas para identificar crianças e adolescentes em risco antes que eles atravessem do universo *online* para o *offline*.

& Exploited Children – ICMEC) define o aliciamento como o processo pelo qual um adulto constrói uma relação com uma criança ou um adolescente para facilitar o contato sexual *online* ou *offline* [43]. Por geralmente ser o precursor de um crime mais sério, estatísticas sobre o alcance do aliciamento *online* por si só são difíceis de se obter. Porém, o impacto nas crianças e nos adolescentes que são vitimizados é profundo.

As vítimas relatam sentir vergonha, perda de confiança, cometer automutilações, sofrer ataques de pânico e sentir uma perda de autoconfiança. Em um relatório recente elaborado pela empresa de telecomunicações sueca Telia, 17% das crianças e dos adolescentes pesquisados disseram que suas fotos haviam circulado em mídias sociais sem o seu consentimento, e 7% disseram que haviam sido chantageados. Uma em cada quatro crianças ou adolescentes disse que havia recebido contatos e mensagens *online* perturbadores, sendo as meninas atingidas com mais frequência do que os meninos [44].

Riscos de conteúdo: pornografia, materiais sobre abuso sexual, violência, extremismo, jogos e apostas

Na era pré-internet, era relativamente fácil impedir crianças e adolescentes de acessarem conteúdos de risco ou inadequados para a idade. Para obter uma licença de funcionamento, locais voltados para adultos tinham de impor uma classificação etária.

Infelizmente, isso não acontece *online*. É muito fácil para crianças e adolescentes encontrarem e visualizarem conteúdos com temática adulta, relacionados a tópicos como apostas, pornografia, materiais sobre abuso sexual e violência.

Atualmente, muitas crianças e muitos adolescentes são regularmente expostos à pornografia adulta no ambiente *online*. Um estudo de 2018 do *Journal of Adolescent Health* identificou que uma em cada cinco crianças ou adolescentes entre 9 e 17 anos vê material sexual *online* indesejado [5].

Outro estudo identificou que quase 40% dos adolescentes desejam reproduzir as práticas sexuais que viram na pornografia *online* [46]. Um estudo de 2017 realizado no Reino Unido identificou que quatro em cada cinco crianças e adolescentes acham que as mídias sociais e as empresas de internet devem fazer mais para protegê-los dos materiais sexuais [47].

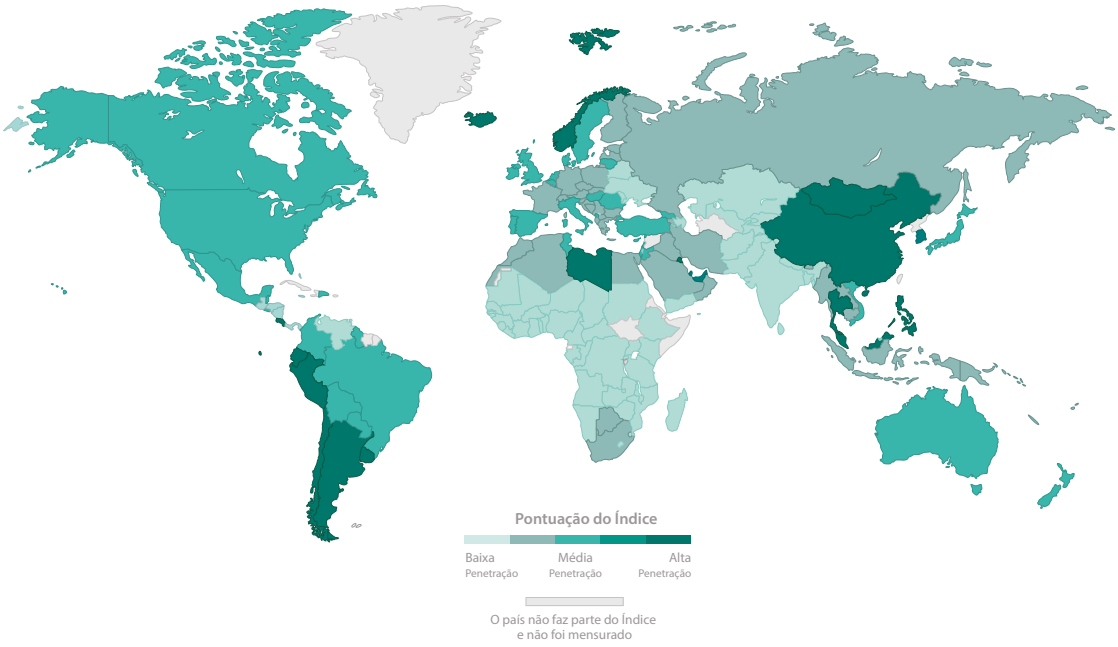
Infelizmente, muitas crianças e muitos adolescentes também estão sendo expostos a discursos de ódio e ao extremismo *online*. Um relatório produzido nos EUA identificou que, em 2018, 27% dos norte-americanos foram alvo de assédio e ódio extremo *online*; e que 38% haviam parado de usar o serviço em questão ou mudaram a forma de utilizá-lo [48].

Crianças e adolescentes também podem ser expostos aos riscos por meio de jogos *online*. Apesar de apresentarem uma classificação por idade, muitos jogos não realizam uma verificação efetiva. Por conta disso, com frequência crianças e adolescentes podem acessar fóruns e *chats* que não são moderados. Também podem ser expostos a conteúdos sexuais inadequados para a idade e a jogos violentos, *bullying* cibernético e aliciamento nos fóruns e nos chats [49].

Uma recente revisão da literatura acadêmica sobre jogos de azar identificou que até 12% dos adolescentes de todo o mundo podem ter problema com apostas [52]. Estudos realizados em diversos mercados, incluindo o Reino Unido, o Canadá, os EUA e países nórdicos identificaram que entre 8% e 34% de crianças e adolescentes com menos de 18 anos em algum momento haviam apostado *online* [53].

Os perigos associados aos viciados em jogos de azar são significativos, entre eles o potencial de se endividar. Um estudo recente identificou que os viciados em jogos de azar tinham uma probabilidade 15 vezes maior, em média, de cometerem suicídio [54].

Índice de Conectividade Móvel GSMA: Penetração das mídias sociais móveis em 2018



Fonte: GSMA Mobile Connectivity Index 2019. GSMA Intelligence Unit

Jovens de vários países de todo o mundo já têm acesso a mídias sociais em dispositivos móveis. Com a expansão da banda larga, a penetração das mídias sociais aumentará rapidamente, expondo mais crianças e adolescentes aos riscos e perigos online.

Por fim, crianças e adolescentes não supervisionados no ambiente *online* em geral correm o risco de ver conteúdos violentos, que podem ser perturbadores, inadequados para a idade ou mesmo que mostram alguma atividade criminosa. Um estudo realizado em 2018 identificou que a exposição a mídias violentas apresenta uma forte correlação com o aumento da suscetibilidade de se desenvolver comportamento antissocial [50].

Um estudo da rede *EU Kids Online* identificou que 18% de crianças e adolescentes disseram estar preocupados com a exposição a conteúdos violentos *online* [51].

Riscos de conduta: uso indevido de dados, abuso financeiro e comportamento inadequado

Muitos serviços são desenvolvidos para ter classificação etária, e geralmente são proibidos para crianças e adolescentes com menos de 13 anos, em conformidade com a Lei de Proteção da Privacidade *Online* de Crianças e Adolescentes dos EUA. Porém, em muitos casos, é extremamente fácil para crianças e adolescentes contornarem essas restrições de idade. Estudos realizados pelo *Pew Center*, nos EUA, e pela Sociedade Nacional para a Prevenção da Crueldade contra Crianças (*National Society for the Prevention of Cruelty to Children* – NSPCC), do Reino Unido, identificaram que, quando atingem 12 anos, cerca de metade das crianças já possui contas em mídias sociais [55] [56].

Os possíveis perigos associados ao uso de mídias sociais por crianças abaixo da idade mínima incluem:

- Baixas taxas de atividade física, o que contribui para um nível de saúde deficiente em crianças e adolescentes [57].
- Interrupções no sono e impactos no bem-estar na escola [58].
- Ansiedade e depressão, que os estudos mostram aumentar com o uso das mídias sociais [59].

Outro risco, com o qual também é muito fácil para crianças e adolescentes se envolverem, são os gastos não pretendidos e não autorizados. Muitos programas oferecem compras em aplicativos, que em geral são bastante promovidos por anúncios dentro do jogo ou aplicativo.

Um estudo recente da Sociedade de Pediatria do Desenvolvimento e do Comportamento identificou que quase todos os aplicativos destinados a crianças e adolescentes contêm anúncios, muitos deles descritos pelos pesquisadores como "manipulativos". Entre outras práticas, a pesquisa observou o uso frequente de anúncios *pop-up* que interrompem o jogo e de personagens do próprio jogo que pedem para que as crianças e os adolescentes efetuem compras, voluntária ou involuntariamente [60].

Riscos de contrato: o quão fundamentado é o consentimento de crianças e adolescentes *online*?

Todos os riscos descritos nas páginas anteriores desta seção se enquadram em um cenário de interações digitais que não são apropriadas para crianças e adolescentes. Um estudo de 2019 realizado por dois professores de direito identificou que 99% dos termos e condições *online* eram escritos com uma linguagem muito complexa para a compreensão do púbico médio, não formado em uma universidade [6].

Não haveria como crianças e adolescentes entenderem o que assinam quando instalam aplicativos ou acessam um *site*. Serviços e obrigações que são desenvolvidos para adultos devem ter limitação de idade, de forma que crianças e adolescentes não possam se inscrever sem a permissão de um responsável. Sem entender o que estão fazendo, crianças e adolescentes podem se inscrever em diversos tipos de monitoramento de dados. Na maior parte dos contextos,

Comissão Infantil do Reino Unido cria termos e condições acessíveis para crianças e adolescentes

Em 2017, a Comissão Infantil do Reino Unido criou versões simples em inglês dos termos e condições para as seguintes plataformas: Facebook, Instagram, Snapchat, YouTube e WhatsApp. Redigidos por advogados, eles foram elaborados para serem fáceis de se entender, de forma que os pais e responsáveis pudessem compreender no que crianças e adolescentes estavam se inscrevendo quando utilizassem algum desses serviços. Você pode encontrar esses termos e condições simplificados aqui:

https://www.childrenscommissioner.gov.uk/publication/simplified-social-media-terms-and-conditions-for-facebook-instagram-snapchat-youtube-and-whatsapp/

as empresas não podem tratar crianças e adolescentes dessa forma.

Contudo, se seus sistemas não priorizam o bem-estar de crianças e adolescentes, elas podem acabar fazendo isso de qualquer maneira.

Enquanto estão *online*, crianças e adolescentes também correm o risco de gastar dinheiro sem a permissão de seus pais ou responsáveis e, assim, ter seus dados coletados. Uma pesquisa recente mostra que 90% dos aplicativos de terceiros na loja Android Play coletam dados do usuário, como idade, sexo, localização e padrões de uso [61].

As "pegadas digitais" de crianças e adolescentes, bem como a capacidade de várias plataformas combinarem e integrarem esses dados para gerar informações, têm o potencial de determinar e causar impactos no futuro deles. Corremos o risco de permitir que crianças e adolescentes de toda uma geração sejam capturados como dados, quantificados, vendidos e revendidos. Esses dados, que poderiam incluir qualquer coisa, desde informações pessoais sensíveis, como data de nascimento, até detalhes da atividade *online* da criança ou do adolescente – coletados sem o consentimento esclarecido destes –, poderiam influenciar as futuras oportunidades de vida de crianças e adolescentes, incluindo seu acesso à educação, a serviços e empregos.
data de nascimento, até detalhes da atividade *online* da criança ou do adolescente – coletados sem o consentimento esclarecido destes –, poderiam influenciar as futuras oportunidades de vida de crianças e adolescentes, incluindo seu acesso à educação, a serviços e empregos.

Um resumo da situação de crianças e adolescentes no ambiente *online*

No mundo todo, crianças e adolescentes muito frequentemente são expostos a perigos e violências devido à falta de monitoramento na internet. Mesmo as crianças e os adolescentes que não se tornam vítimas de comportamentos predatórios de adultos geralmente se encontram em desvantagem, pelas ações e omissões dos serviços e produtos que não levam em conta suas necessidades, ou que não tomam medidas suficientes para protegê-los [23].

Oportunidades

6

Oportunidades

Estamos passando por uma transformação digital de âmbito global. Isso não apenas promete trazer diversos benefícios para crianças e adolescentes – por exemplo, maior acesso a oportunidades educacionais, culturais e econômicas –, como também há sinais encorajadores de que as mudanças tecnológicas e sociais que ela traz revolucionarão a luta contra a exploração e o abuso sexual de crianças e adolescentes no ambiente *online*.

A inteligência artificial e a luta contra a violência sexual de crianças e adolescentes *online*

O desenvolvimento da inteligência artificial (IA) tem o potencial de ajudar empresas e autoridades a analisarem mais materiais sexuais que envolvem crianças e adolescentes suspeitos ou outros conteúdos de abuso sexual, assim como a identificar de forma mais exata materiais ilegais, agressores e vítimas com maior frequência e agilidade.

Em 2018, o Google anunciou a introdução de uma nova rede neural profunda para melhorar a detecção de materiais sexuais que envolvem crianças e adolescentes. Em testes, a empresa reportou que o uso da IA ajudou a melhorar a detecção e as taxas de relatos em 700% [62].

A Microsoft da Alemanha está trabalhando com a polícia nacional para desenvolver uma IA que seja capaz de identificar mais rapidamente materiais sexuais que envolvem crianças e adolescentes [63], assim como ocorre com as autoridades nos Países Baixos [64], na Austrália [65] e no Reino Unido [66]. A ferramenta *Griffeye Brain* é uma IA de classificação que analisa materiais não examinados, para sugerir arquivos que julga retratar abuso sexual de crianças e adolescentes. Essa ferramenta ajuda a acelerar as investigações e destaca materiais de abuso sexual de crianças e adolescentes que não eram conhecidos anteriormente [67].

A polícia do Reino Unido também está utilizando IA para encontrar e identificar conteúdo extremista *online* do tipo utilizado para recrutar crianças e adolescentes para movimentos radicais [68]. O Facebook está construindo um sistema de IA para identificar não somente materiais sobre abuso sexual de crianças e adolescentes, mas também conversas que incluem sinais reveladores de aliciamento [69].

No início de 2019, a Microsoft organizou um *hackathon* para trabalhar com a *WeProtect Global Alliance* (WPGA), que reuniu engenheiros e especialistas jurídicos e operacionais da Microsoft, do Google, do Facebook, do Snapchat e do Twitter para desenvolver uma ferramenta de IA para enfrentar o aliciamento *online* [70]. Nos EUA, a Marinus Analytics desenvolveu um *software* de IA que pesquisa anúncios *online* de serviços sexuais para identificar vítimas de tráfico e coletar evidências para ajudar a polícia a levar os traficantes à Justiça [71].
A Thorn implementou tecnologia de IA em sua ferramenta de investigação sobre tráfico sexual de crianças e adolescentes, o Spotlight, para oferecer às autoridades de todos os 50 estados dos EUA e do Canadá a capacidade de acelerar a identificação das vítimas e reduzir o tempo de investigação em mais de 60% [72].

Na conferência *Code* 8.7 de 2019, intitulada "Utilizar a ciência da computação e a IA para acabar com a escravidão moderna", os participantes levantaram a possibilidade de criar um banco de dados comum de vítimas – como o banco de dados de Exploração Sexual de Crianças e Adolescentes da Interpol – ou de traficantes, acessível às autoridades de todo o mundo [73]. Embora não chame tanta atenção quanto a IA ou as tecnologias emergentes, essa seria uma grande etapa tecnológica na luta contra o tráfico de crianças e adolescentes.

Também há planos de utilizar a IA para combater o *bullying* cibernético e o assédio *online*. Recentemente, o Instagram lançou uma ferramenta de IA para detectar e impedir o assédio *online* em sua fase inicial [74]. Na Europa, um projeto da União Europeia chamado *Creep* utiliza a IA para indicar *bullying* cibernético e mostrar a diferença entre o *bullying* e uma simples desavença [75].

Outras tecnologias emergentes

Outras tecnologias emergentes também têm o potencial de ajudar na luta contra os perigos *online* para crianças e adolescentes. No Capítulo 4, vimos as tecnologias como bloqueios por lista, filtros heurísticos e o uso de *web crawlers* para encontrar, detectar, relatar e bloquear materiais sexuais que envolvem crianças e adolescentes, e outras formas de conteúdo sobre abuso sexual de meninas e meninos. Essas tecnologias não são novas, mas ainda não estão sendo amplamente utilizadas.

Outras tecnologias realmente novas que estão sendo utilizadas no enfrentamento ao abuso sexual de crianças e adolescentes no ambiente *online* incluem:

- Tecnologia de reconhecimento facial aprimorado, que ajuda a identificar mais rapidamente crianças e adolescentes vítimas de exploração sexual [76].
- Maior poder de processamento e melhor reconhecimento de imagens, que permitem que um HD de 1TB suspeito seja examinado em apenas 30 minutos para identificar conteúdo ilegal previamente conhecido [77].
- Dados de análise preditiva sendo utilizados por autoridades para identificar crianças e adolescentes em situação de risco de abuso sexual, e para intervir antes que as violações aconteçam [78].

Conforme essas e outras novas tecnologias vão amadurecendo, haverá muitas oportunidades para que as empresas as utilizem na luta contra os danos causados a crianças e adolescentes no ambiente *online*. E ainda mais: o simples fato de um país estar conectado à internet pode simplificar e acelerar a cooperação entre suas autoridades e empresas com as de outros países.

Cooperação internacional crescente

Desde 2008, a UIT lançou a Iniciativa *Child Online Protection* (COP), como um esforço entre múltiplos *stakeholders* dentro da estrutura da Agenda Global de Segurança Cibernética (*Global Cibersecurity Agenda* – GCA). Essa iniciativa reúne parceiros de todos os setores da comunidade global para criar uma experiência *online* mais segura e empoderadora para crianças e adolescentes em todo o mundo. E, ao longo dos anos, a iniciativa vem levantando de forma contínua a questão para a comunidade internacional.

Outro progresso animador foi o aumento da cooperação entre países e entre setores para encontrar soluções comuns na luta contra a violência sexual de crianças e adolescentes *online*. Iniciativas globais recentes incluem a *WeProtect Global Alliance* e a *Child Dignity Alliance*.

Cada vez mais, as autoridades também estão trabalhando através das fronteiras. Na Operação Tantalio, de 2017, a Interpol, a Europol e as autoridades de 15 países cooperaram para prender 39 indivíduos e acabar com uma rede *online* de distribuição de materiais sexuais envolvendo crianças e adolescentes [79]. Em 2019, Austrália, Bulgária, EUA, Nova Zelândia e Tailândia trabalharam em conjunto para prender e processar agressores na Tailândia, na Austrália e nos EUA, assim como resgatar 50 crianças e adolescentes [80].

Também há uma colaboração crescente entre as linhas diretas de denúncia, ISPs e autoridades. Por meio de sua plataforma segura ICCAM, financiada pela Comissão Europeia, a INHOPE obtém dicas por meio das linhas de denúncia de todo o mundo e toma ações para remover materiais sexuais que envolvem crianças e adolescentes em qualquer país participante. Uma prova do valor dessa abordagem é o fato de que 60% dos vídeos descobertos pela ICCAM em 2017 não eram conhecidos anteriormente pelos órgãos judiciais internacionais [81].

7

Ameaças e o ambiente ameaçador

Ameaças e o ambiente ameaçador

Exploração, abuso sexual e sistemas mal desenvolvidos que expõem crianças e adolescentes a riscos desnecessários são muito comuns no ambiente *online*. E esses perigos não acontecem isoladamente. Eles são possibilitados por uma série de fatores técnicos, sociais e legais. Para proteger crianças e adolescentes *online*, é importante entender os riscos que eles enfrentam e os fatores por trás desses riscos.

Empresas e outros órgãos poderiam facilmente minimizar alguns riscos na etapa de *design*. Poderiam, por exemplo, acabar com a localização em tempo real de crianças e adolescentes disponível para outros usuários, integrar a segurança a partir da origem em dispositivos inteligentes para a casa (de modo a impedir o *streaming* por acidente), integrar a verificação de idade e o *design* pensado para crianças e adolescentes em seus produtos e serviços e, por fim, reduzir o uso de gatilhos competitivos, que incentivam comportamentos de risco.

Outro fator-chave que contribui para o nível de risco que crianças e adolescentes enfrentam *online* é a falta de mecanismos efetivos e robustos (incluindo legislação apropriada), por meio dos quais o Estado e a sociedade civil podem responsabilizar aqueles que buscam ativamente explorar ou abusar sexualmente de crianças e adolescentes *online* [83].

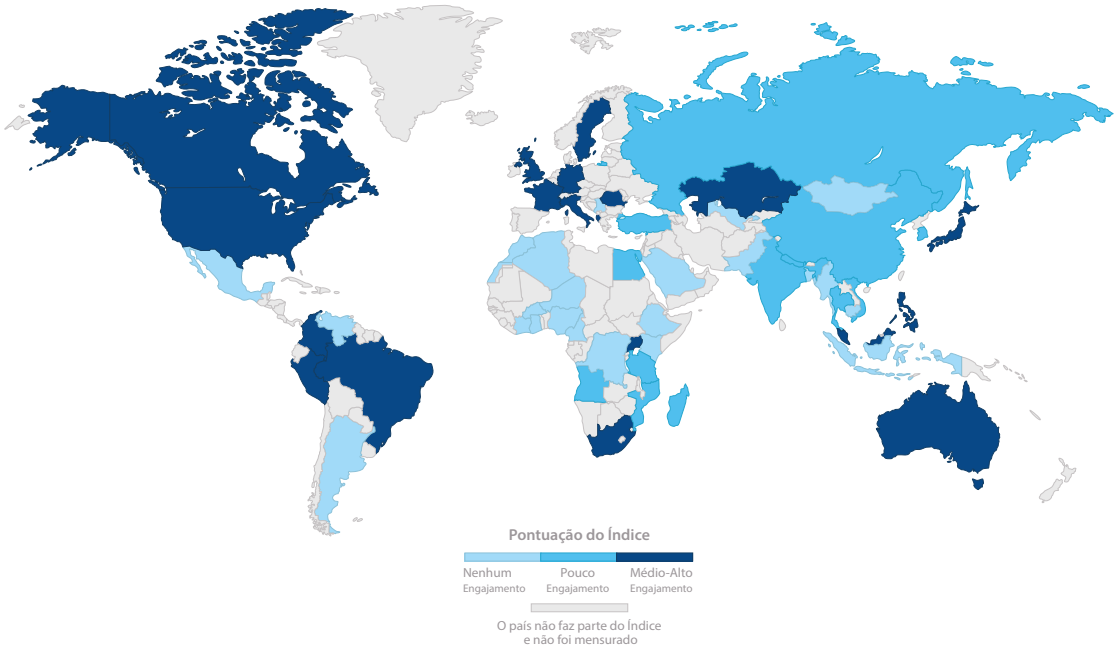
O Índice Fora das Sombras (*Out of Shadows Index*) da EIU

O Índice Fora das Sombras [83], desenvolvido pela *Economist Intelligence Unit* (EIU), realizou um estudo com 60 países (abrangendo 85% das crianças e dos adolescentes do mundo todo) para avaliar sua capacidade de resposta à violência sexual contra crianças e adolescentes, incluindo no ambiente *online*.

Os dados desse estudo foram utilizados para criar um índice, com um escopo em que 100 indica o nível mais alto de proteção, e 0, o menor. Entre outras conclusões, a EIU identificou que:

- Nenhum país está fazendo o suficiente, e apenas quatro países pontuaram acima do 75º percentil.
- 11 países ficaram abaixo de 50 pontos no quesito relativo ao ambiente protetivo que oferecem a crianças e adolescentes.
- 16 países ficaram abaixo de 50 pontos no quesito relativo à qualidade de sua base legal de proteção a crianças e adolescentes.
- 36 países ficaram abaixo de 50 pontos no quesito relativo ao engajamento da sociedade civil e do setor privado.
- 37 países ficaram abaixo de 50 pontos no quesito relativo à sua capacidade legal de proteger crianças e adolescentes.

Engajamento da indústria: resposta à violência sexual contra crianças e adolescentes *online*



Fonte: Out of the shadows: shining light on the response to child sexual abuse and exploitation. The Economist Intelligence Unit. 2019.

Dos 60 países analisados pela EIU, em apenas 10 havia mecanismos de comunicação do setor de tecnologia que eram usados ativamente para reportar a violência sexual contra crianças e adolescentes no ambiente online.

Os países de renda média e baixa apresentam capacidades e recursos tecnológicos bem menos desenvolvidos para impedir ou investigar crimes *online*. Mesmo os países de renda alta podem não ter estratégias para crimes cibernéticos.

Além disso, em alguns casos, as leis podem não ter sido atualizadas para incluir crimes específicos e instrumentos relevantes para investigar e processar os crimes cibernéticos [82]. A tecnologia se transforma mais rápido que legisladores e autoridades conseguem acompanhar, o que deixa brechas por onde podem passar inovações negligentes ou agressores.

Falhas nas políticas e nas leis nacionais

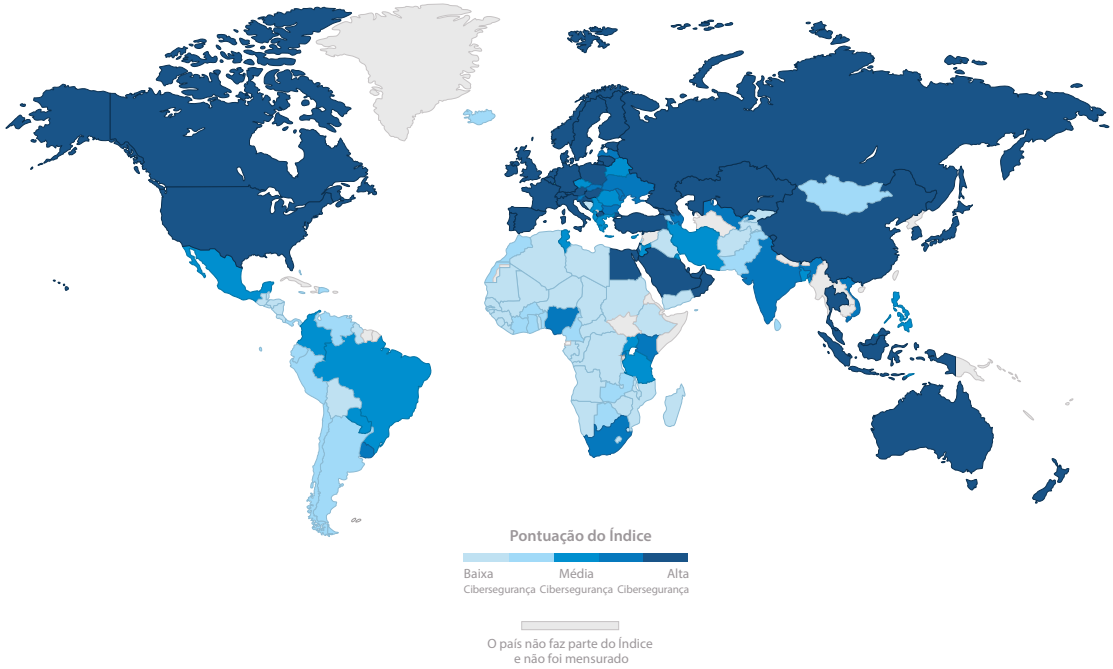
Conforme a sociedade passa por uma rápida transformação digital, existe um risco de que novas tecnologias e abordagens sejam colocadas em prática sem considerar de forma apropriada o impacto nos membros mais vulneráveis da sociedade – particularmente no caso de crianças e adolescentes.

Muitos países não têm, em seus planos nacionais de banda larga, seções sobre as necessidades e os direitos de crianças e adolescentes. Isso aumenta a probabilidade de que as entidades públicas e privadas criem políticas, plataformas e serviços que não sejam, por *design*, adequados e seguros para crianças e adolescentes.

Para tratar desse problema, o UNICEF, o Pacto Global da ONU e a *Save the Children* estabeleceram os Direitos e Princípios Comerciais de Crianças e Adolescentes [84]. Esse instrumento proporciona um conjunto de princípios claros e práticos que as organizações podem seguir para respeitar crianças e adolescentes, bem como seus direitos, em cada aspecto de suas atividades.

Você pode encontrar os princípios aqui: https:// www.unicef.org/csr/theprinciples.html

Índice de Conectividade Móvel GSMA: Índice de Cibersegurança



Fonte: GSMA Mobile Connectivity Index 2019. GSMA Intelligence Unit

No Índice de Conectividade Global GSMA, muitos dos países com as menores taxas de segurança cibernética também são aqueles com maior concentração de população com menos de 19 anos de idade.

Para ver um estudo de caso sobre como a legislação e a política nacionais podem ser reformuladas de forma satisfatória para proteger e aprimorar os direitos *online* de crianças e adolescentes, consulte a página 77, que resume o trabalho realizado pelo governo de Ruanda e seus parceiros.

As leis de segurança cibernética devem ser modernizadas

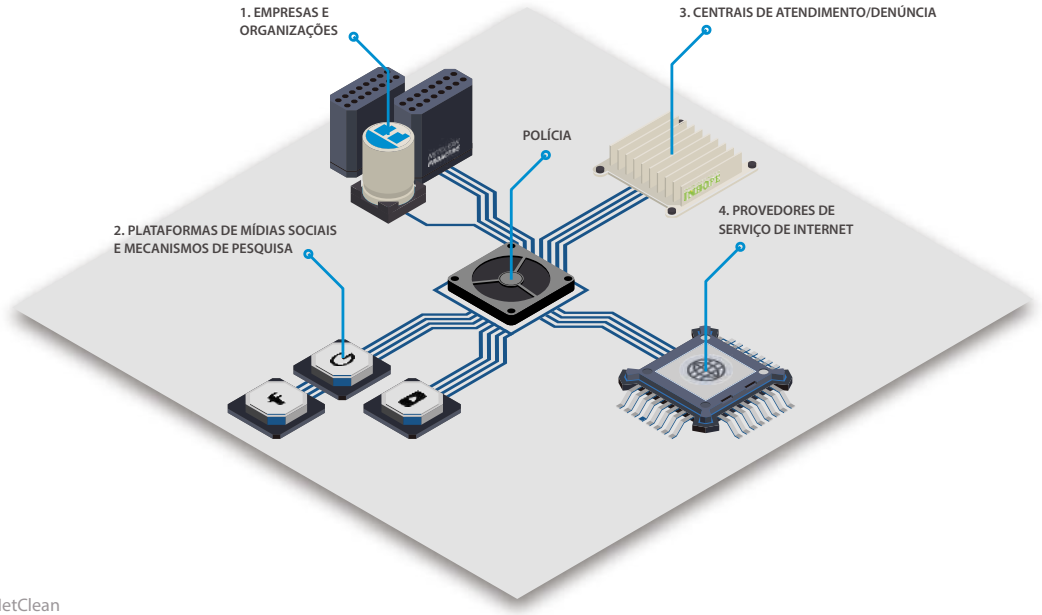
Hoje, apenas 72% dos países apresentam uma legislação funcional para crimes cibernéticos [85]. Mesmo nas próprias nações, com frequência falta consistência legal e nas definições operacionais sobre o que constitui perigo para crianças e adolescentes *online*, assim como faltam ações coordenadas entre diferentes agências. Essa conduta permite que os agressores que atuam em territórios com bases legais fracas distribuam materiais sexuais envolvendo crianças e adolescentes e tenham impunidade no mundo todo.

No Índice de Conectividade Global GSMA, muitos dos países com as menores taxas de segurança cibernética também são aqueles com maior concentração de população com menos de 19 anos de idade.

Para lidar com isso, os países devem adotar leis de segurança cibernética rigorosas e que sejam aplicadas de forma consistente por forças policiais com recursos, motivação e devidamente equipadas. Considerando a natureza sem fronteiras da exploração e do abuso sexual de crianças e adolescentes no ambiente *online*, também é importante reconhecer que a proteção deles é uma questão global, que requer cooperação internacional, classificações e marcos legais harmonizados de acordo com as diretrizes da UIT COP e do UNICEF COP para a indústria [86].

Apenas com normas e classificações acordadas em âmbito internacional os Estados serão capazes de compartilhar

Fluxo de cooperação



Fonte: NetClean

Para ter sucesso em identificar os agressores, remover materiais sobre abuso sexual de crianças e adolescentes, e ajudar as vítimas, todos os stakeholders devem trabalhar em conjunto e conhecer seus respectivos papéis.

os dados e agrupar os recursos para enfrentar o abuso sexual de crianças e adolescentes no ambiente *online*.

Falta de sistemas de responsabilização e normas obrigatórias

Tornar a internet um espaço mais seguro para ser navegado é mais fácil de se fazer quando os reguladores e as autoridades conseguem trabalhar de perto com os prestadores de serviço de internet (ISPs), operadoras de rede móvel, ferramentas de busca, instalações de internet pública e agências similares. Essas empresas têm a capacidade de detectar materiais sobre abuso sexual de crianças e adolescentes na fonte e encaminhar às autoridades os detalhes relevantes. Contudo, para fazer isso, elas precisam de leis e procedimentos que deixem claro seu papel e suas responsabilidades nesse processo.

Entretanto, menos de um em cada seis países estabeleceu em sua legislação o relato obrigatório de ISPs, o bloqueio e a exclusão de conteúdo, e o armazenamento de registros. Mais de 40% dos países não possuem uma legislação a esse respeito. Outro obstáculo significativo é a falha nas definições de origem (*by default*) e a falta de adesão às diretrizes de Luxemburgo, o que dificulta a coordenação do combate internacional à exploração e ao abuso sexual de crianças e adolescentes [87].

A necessidade de entender e rastrear os agressores

Além de encontrar e acabar com os *sites* e serviços que os agressores utilizam para cometer seus crimes, também é necessário identificar e entender os criminosos em si. Isso é essencial se quisermos impedir que agressores conhecidos voltem a vitimizar crianças e adolescentes, e também se quisermos aprender a identificar criminosos em potencial e agir antes que cometam um crime.

Porém, com frequência, os agressores não são identificados nem punidos. E mesmo quando são detectados e responsabilizados, concluiu-se que até 8% dos condenados por crimes relacionados ao contato com crianças e adolescentes voltam a cometer o crime [88].

Para aumentar as taxas de identificação de agressores e reduzir o risco de os condenados voltarem a cometer o crime, é necessário ter um maior conhecimento do que caracteriza e motiva os agressores – para crimes de materiais sexuais que envolvem crianças e adolescentes, assim como para outros tipos de violações *online*, incluindo o *bullying* cibernético, o assédio e o recrutamento de crianças e adolescentes por movimentos radicais.

Em 2018, a Thorn, em parceria com o NCMEC, publicou um relatório que examinou as tendências nos materiais sexuais que envolvem crianças e adolescentes comercializados ativamente. Entre outros achados, esse relatório identificou que os homens que produzem desse tipo de conteúdo eram em número muito maior que as mulheres. Os casos que envolviam produtoras do sexo feminino normalmente retratavam abuso sexual familiar de crianças mais novas. Além disso, a pesquisa identificou que o material sobre abuso sexual de crianças e adolescentes distribuído está se tornando cada vez mais violento, com mais casos retratando penetração do que dez anos atrás [89]. De acordo com uma pesquisa da NetClean, o produtor comum de materiais sexuais que envolvem crianças e adolescentes é homem, sendo que mais de 50% dos policiais nunca encontraram uma agressora do sexo feminino [90].

Desenvolver ideias como essas é essencial para ajudar as autoridades a alocar seus escassos recursos em ações calculadas para ter o maior impacto possível. E considerando o crescimento dos *sites* na *darknet*, que são muito mais difíceis e mais caros de se investigar, impedir a primeira ocorrência e as repetições dos crimes pode ter um impacto imenso na escala das tarefas realizadas pelas autoridades policiais.

Recentemente, ocorreu o surgimento de centrais de ajuda do tipo *Stop It Now* [Pare Agora], que oferecem orientação e ajuda gratuita e anônima, por telefone ou *chat*, para pessoas que vivenciaram sentimentos ou pensamentos de interesse sexual por crianças e adolescentes – ou seja, potenciais agressores [91].

Uma gama de ameaças provenientes do uso indevido da tecnologia

No início da internet, murais de mensagens de fóruns de discussão eram um dos vetores mais importantes para a distribuição de materiais sobre abuso sexual de crianças e adolescentes. Com o crescimento da rede mundial de computadores, muito desses materiais e de outros conteúdos sobre abuso sexual migraram dos fóruns de discussão para ser abrigados em *websites*.

Em meados da década de 2000, as autoridades e os provedores se tornaram cada vez mais conscientes do problema dos *sites* que hospedam esse tipo de material, e também se tornaram mais efetivos em desativar *sites* e processar os publicadores e os usuários que os acessam.

Isso fez com que muitos agressores migrassem sua atividade para serviços de compartilhamento de arquivos *peer-to-peer* (P2P). O volume do tráfego das redes P2P dificultou a fiscalização desse problema – o que piorou ainda mais pelo uso crescente de criptografia. As mídias sociais também são populares entre os criminosos, pois são canais para tomar crianças e adolescentes como alvo e trocar informações entre si. Para ser efetivo no trabalho de detectar a exploração e o abuso sexual, ajudar crianças e adolescentes e responsabilizar os agressores, sempre devemos tratar de todas as ameaças e de todo o ambiente

ao redor das ameaças. A Avaliação Mundial de Ameaças da *WeProtect Global Alliance* de 2018 identifica os seguintes fatores, entre outros, como sendo complicações significativas no combate à exploração e ao abuso sexual de crianças e adolescentes no ambiente *online*:

- O acesso à internet de alta velocidade capacita os agressores e o compartilhamento de materiais sexuais que envolvem crianças e adolescentes.
- A crescente disponibilidade de mensagens criptografadas ajuda os agressores a se comunicarem de forma secreta.
- O uso de redes privadas virtuais (*virtual private networks* – VPNs) facilita o ocultamento das ações dos criminosos.
- Os custos de produção de mídias interativas, como vídeos e fotos de alta resolução, estão caindo cada vez mais.
- A tecnologia de manipulação de fotos falsas (*deepfake*) facilita a criação e a ocultação de material sexual envolvendo crianças e adolescentes.
- A transmissão ao vivo (*livestreaming*) permite o compartilhamento instantâneo e único de materiais sexuais de crianças e adolescentes, o que é difícil para as autoridades detectarem.
- O armazenamento na nuvem (*cloud storage*) de baixo custo facilita aos agressores armazenarem e compartilharem material sexual que envolve crianças e adolescentes *online*.
- O armazenamento USB é tão barato atualmente que a transferência de materiais sobre abuso sexual de crianças e adolescentes se tornou muito fácil. Com frequência, esses *drives* são protegidos por leis de privacidade de dados mais rígidas do que as leis que protegem crianças e adolescentes.

A criptografia e outras tecnologias que promovem o anonimato são cada vez mais comuns e apresentam um desafio significativo para o enfrentamento do problema da exploração e abuso sexual de crianças e adolescentes no ambiente *online*, tanto para as autoridades policiais quanto para outras entidades.
A criptografia torna impossível a detecção de materiais sobre abuso sexual de crianças e adolescentes até que o arquivo seja descriptografado, quando chega ao destinatário da mensagem que foi criptografada. Para tratar desse problema, é essencial que a legislação determine que os ISPs tenham acesso a soluções de perícia de imagens que permitam o exame de fotos e vídeos de materiais sexuais que envolvem crianças e adolescentes.
As soluções que podem ser adotadas incluem o PhotoDNA, utilizado atualmente por muitas empresas de tecnologia.
As autoridades também enfrentam o desafio dos espaços de armazenamento criptografados, que demandam muito esforço e conhecimento técnico ter seus conteúdos acessados. Os legisladores devem tratar desses desafios priorizando os direitos de crianças e adolescentes, ao mesmo tempo em que asseguram a não violação ao direito à privacidade.

Como as lacunas na tecnologia possibilitam a exploração e o abuso sexual

Já existem *softwares* e soluções para ajudar empresas privadas, órgãos reguladores e autoridades legais a identificar, reportar e agir contra os *sites* e serviços que abrigam materiais sobre abuso sexual de crianças e adolescentes. Muitas dessas soluções são extremamente automatizadas e utilizam algoritmos *hash* para minimizar a exposição da equipe a conteúdos prejudiciais. Muitos estão disponíveis com custo baixo ou de forma gratuita.

Para vencer a luta contra a exploração e o abuso sexual *online*, todas as agências

e organizações pertinentes – incluindo empresas que prestam serviços *online* – devem usar todas as tecnologias disponíveis para suprir as lacunas tecnológicas que facilitam a atuação dos agressores no ambiente *online*.

Exemplos dos tipos de pacotes tecnológicos disponíveis incluem:

- **NetClean ProActive –** *software* com base na correspondência de assinatura e em outros algoritmos de detecção, que identifica automaticamente imagens e vídeos de abuso sexual de crianças e adolescentes em ambientes empresariais.

- **Thorn's Safer –** ferramenta que pode ser implementada diretamente em uma plataforma empresarial privada para identificar, remover e reportar materiais sexuais que envolvem crianças e adolescentes.

- **Griffeye Brain –** IA que examina conteúdos não classificados anteriormente, compara-os com os atributos de materiais sexuais conhecidos que envolvem crianças e adolescentes e indica automaticamente itens suspeitos para revisão de um agente.

- **PhotoDNA –** ferramenta que cria *hashes* de imagens e as compara com um banco de dados de *hashes* já identificados e confirmados como sendo materiais de abuso sexual de crianças e adolescentes. Se encontrar uma correspondência, a imagem é bloqueada.

Para uma lista mais completa de *softwares*, consulte a seção de "Recursos" no final deste relatório.

Devemos observar que os planos de diversas empresas de internet de implementar criptografia de ponta a ponta em seus serviços, incluindo em navegadores populares, plataformas de mídias sociais e serviços de mensagem, ameaçam inutilizar as ferramentas desenvolvidas para enfrentar e coibir a distribuição de materiais sexuais que envolvem crianças e adolescentes. Essas ferramentas não são compatíveis perfeitamente com a criptografia de ponta a ponta. Portanto, os *stakeholders* – públicos e privados – devem tomar medidas concretas para assegurar que a criptografia seja implementada de uma forma que permita que as ferramentas continuem a operar.

O crescimento da *darknet*

O termo *darknet* se refere a *sites* e serviços que, mais do que estarem apenas fora de vista, são ocultados de forma intencional com o uso de ferramentas e protocolos de criptografia. A melhor estimativa disponível até o momento diz que há cerca de 8,5 mil *sites* na *darknet*, acessíveis com o uso do navegador criptografado e anônimo Tor [92]. De acordo com uma pesquisa realizada em 2019, aproximadamente 100 desses *sites* são lojas nas quais produtos ilegais, possivelmente materiais sobre violência sexual contra crianças e adolescentes, estão disponíveis para venda [92].

Os *sites* da *darknet* podem ser lojas simples, ou podem atuar como comunidades *online* nas quais os criminosos criam um senso de normalidade compartilhado, permitindo e encorajando as atividades uns dos outros. Isso estimula os agressores a cometerem crimes cada vez mais graves. Juntamente com a disponibilidade de telefones com câmeras baratos e de alta qualidade, a *darknet* é uma das principais plataformas de exploração e abuso sexual *online* nos dias de hoje.

De acordo com um estudo citado pela *ECPAT Internacional*, apenas 2% dos *sites* na *darknet* abrigam material sobre abuso sexual de crianças e adolescentes, mas esses poucos *sites* são responsáveis por 80% de todo o tráfego na *darknet* [93].

O papel do contexto social e cultural de crianças e adolescentes

Crianças e adolescentes são, por natureza, vulneráveis àquelas pessoas que são responsáveis por sua segurança. Porém, ao mesmo tempo em que o abuso sexual de crianças e adolescentes nunca é de responsabilidade deles próprios, há muitos fatores presentes em seu ambiente e em sua criação que podem aumentar sua vulnerabilidade a sofrer tais violações.

Uma criança ou um adolescente criado em uma cultura na qual segredos são encorajados, que é exposto a materiais sexuais ou que testemunha situações na qual sexo é trocado por dinheiro, drogas ou proteção, pode se tornar menos capaz de entender a violação sexual como algo inaceitável. Uma criança ou um adolescente exposto à violência ou ao controle opressivo – ou que tem medo de figuras de autoridade – pode ter dificuldade em buscar proteção [94].

Negligência, isolamento emocional ou deficiência podem causar baixa autoestima e uma autoimagem ruim. Isso, por sua vez, pode fazer com que a criança ou o adolescente não se veja como merecedor de proteção [95]. Geralmente, um dos principais fatores disso é uma ligação fraca ou ausente com um adulto de referência confiável. Crianças e adolescentes sem uma base de proteção – fugitivos, por exemplo –, correm um risco particular, assim como aqueles que vivem em casas de acolhimento, ou crianças e adolescentes com deficiências [96].

As normas socioculturais, incluindo a vergonha e o medo, também são fatores importantes em permitir que a exploração e o abuso sexual passem despercebidos. Ameaças contra a criança ou o adolescente, ou contra outras pessoas com as quais eles se importam, podem levar a uma atmosfera de segredos. A vergonha e o medo de serem julgados também podem impedir que crianças e adolescentes revelem essas agressões [97].

Outros fatores que podem aumentar o risco de violência sexual incluem:

- O isolamento social como resultado de um tempo excessivo conectado *online*.
- A falta de verificação de idade, o que permite que crianças e adolescentes acessem conteúdo adulto e fóruns inadequados.
- A sexualização de crianças e adolescentes na cultura como um todo.

O problema tem um escopo muito mais amplo do que apenas a influência de alguns "maus agentes". Inclui todos os fatores que influenciam o comportamento *online* de uma criança ou de um adolescente e a habilidade dele para acessar materiais e fóruns não seguros. Também inclui as atitudes dos adultos na vida da criança ou do adolescente, e a natureza das estruturas nas quais esses adultos estão inseridos. Essas estruturas impedem ou facilitam a violência sexual?

O ambiente social não é apenas um fator na vulnerabilidade de uma criança ou um adolescente relativamente à exploração e ao abuso e sexual: ele também determina o quanto uma criança ou um adolescente está seguro em relação a todos os riscos e perigos *online*, incluindo o aliciamento, o recrutamento por movimentos extremistas e a exploração econômica.

As responsabilidades dos principais *stakeholders*

Muitas pessoas têm a responsabilidade de criar e sustentar crianças e adolescentes enquanto caminham para a vida adulta – por exemplo, pais, responsáveis, famílias, educadores, profissionais de saúde, líderes comunitários, autoridades legais e o setor privado. Porém, muitas dessas pessoas têm pouco ou nenhum treinamento sobre como proteger crianças e adolescentes contra os riscos e perigos no ambiente *online*.

O Estado deve assegurar que todos esses *stakeholders* possam cumprir sua função como protetores e saibam como desempenhar seu papel de manter crianças e adolescentes seguros contra o risco no ambiente *online*, bem como ajudar os jovens a obter total proveito das oportunidades educacionais, econômicas e culturais que a internet oferece.

As principais ações de apoio aos *stakeholders* incluem:

- Priorizar seu treinamento e investir o tempo e o orçamento adequados.
- Conscientizar educadores, pais e responsáveis sobre os riscos *online* e sobre o que fazer para minimizá-los.
- Treinar os prestadores de serviços destinados a crianças e adolescentes para identificar quando uma possível situação de abuso sexual estiver acontecendo e, assim, interferir nela.
- Conceder às autoridades legais poderes, tecnologia e a *expertise* de que precisam.

O papel do setor privado

8

O papel do setor privado

A grande maioria da principal infraestrutura e dos serviços que usamos *online* todos os dias foram construídos e são administrados por empresas privadas. Para se obter sucesso em qualquer esforço para proteger as crianças e os adolescentes *online* é necessário o apoio e o total comprometimento do setor privado. As empresas também devem se comprometer em financiar de forma apropriada ambos seus próprios esforços e esforços coletivos para enfrentar o abuso e a exploração sexual de crianças e adolescentes no ambiente *online*.

As empresas querem fazer a coisa certa pelas crianças e adolescentes que utilizam seus serviços. Contudo, os resultados geralmente deixam muito a desejar. Em 2018, em apenas seis meses, a polícia do Reino Unido registrou 1.944 casos de aliciamento (*grooming*) apenas no Instagram [98]. No início de 2019, foi evidenciado que agressores estavam usando os comentários do Youtube para entrar em contato com crianças e adolescentes [99]. De acordo com uma pesquisa realizada por uma instituição *antibullying*, 37% dos adolescentes que responderam disseram que já haviam sofrido *bullying* no Facebook [100].

Como o setor privado pode melhorar sua abordagem com relação à segurança *online* de crianças e adolescentes? Para responder a esta questão, o Grupo de Trabalho pesquisou alguns dos líderes na área. Eis o que a pesquisa nos mostrou:

- Empresas e ONGs que zelam pela proteção *online* de crianças e adolescentes baseiam sua abordagem em marcos de ação bem estabelecidos, por exemplo, o *WeProtect Model National Response Framework*, ou os *Children's Rights and Business Principles* (CRBP), desenvolvidos pela Save the Children, UNICEF e Global Compact da ONU.
- Os líderes utilizam diversas tecnologias, desde a detecção, filtragem e bloqueio até tecnologias emergentes, como a inteligência artificial.
- Políticas e estratégias de proteção de crianças e adolescentes são desenvolvidas em coordenação e consultoria com diversos *stakeholders* internos e externos, incluindo governo, sociedade civil, crianças e adolescentes.
- Políticas e estratégias devem enfrentar a cultura e o uso cotidiano dos serviços digitais que normalizam os comportamentos sexuais ou de risco, ou que rotineiramente colocam as crianças e adolescentes em ambientes desenvolvidos para adultos. Deve ser mostrado maior comprometimento em proteger os dados e a reputação das crianças e adolescentes, além de proporcionar experiências e espaços apropriados para a idade [23].
- As estratégias possuem metas claras e mensuráveis. Isso não apenas torna possível determinar o sucesso, como também torna mais fácil para os *stakeholders* se engajarem nas campanhas.
- Divulgação e a educação também têm um papel importante na prevenção efetiva. Os exemplos incluem a plataforma DQ #DQEveryChild e a campanha #SafetoLearn da EndViolence.
- Quando ocorrem gargalos e obstáculos, os líderes em proteção de crianças e adolescentes no ambiente *online* se envolvem de maneira ativa com os regulamentadores e outros *stakeholders* para superar esses obstáculos.
- O sucesso das políticas e das campanhas de proteção de

crianças e adolescentes *online* é rastreado e medido. E as métricas são compartilhadas com todos os principais *stakeholders*.

Embora todas as organizações envolvidas tenham reconhecido que a segurança *online* de crianças e adolescentes é um processo contínuo de aprendizagem, sua busca pelas melhores práticas as coloca entre as líderes na área. Entre os participantes estão a Airtel, America Movil, DQ, Facebook, *Global Partnership to End Violence Against Children,* Ericsson, ITU, IWF, *Kenyatta University,* Microsoft, *Moore Center,* NetClean, Samena, Telia, UKE, UNESCO, UNICEF, WPGA e Zain.

A oferta de talentos em tecnologia no mercado de trabalho é extremamente pequena em quase toda parte do mundo.

Nos Estados Unidos, a economia precisa de mais 150 mil profissionais habilidosos na área de tecnologia além dos que já estão disponíveis [101]. Na Europa, esse número se eleva para 420 mil [102]. Já na região da Ásia-Pacífico, são necessários um milhão desses profissionais [103].

Em um ambiente tão competitivo, o setor público e outras organizações dedicadas a enfrentar o abuso sexual *online*, geralmente, têm dificuldade em atrair talentos tecnológicos necessários para ficar à frente de agressores e criminosos *online* que atuam de forma cada vez mais inovadora, motivada e com bons recursos financeiros.

Algumas empresas privadas – incluindo Facebook, Snapchat, Twitter e Google [70] – trabalham em estreita colaboração com autoridades da lei, governos e ONGs

Seis maneiras de como o setor privado pode ajudar a combater o abuso sexual *online* de crianças e adolescentes

Há muitas formas pelas quais o setor privado pode contribuir na luta contra o abuso sexual de crianças e adolescentes no ambiente *online*. Aqui destacamos apenas seis que poderiam fazer uma verdadeira diferença:

1. Assegurar que seus sistemas e serviços para crianças e adolescentes sejam seguros desde seu *design*.

2. Ter funções para moderar e denunciar que sejam proeminentes e munidas de bons recursos.

3. Fornecer talentos de engenharia e programação para desenvolver tecnologias contra o abuso sexual.

4. Trabalhar em estreita colaboração com as autoridades da lei para combater o abuso e a exploração sexual com maior celeridade.

5. Trabalhar com os reguladores e investigadores financeiros para rastrear o fluxo de dinheiro proveniente de abusos.

6. Trabalhar para educar professores, pais e responsáveis para ajudá-los a manter crianças e adolescentes mais seguros do perigo *online*.

para desenvolver ferramentas e abordagens a fim de enfrentar o abuso e a exploração sexual de crianças e adolescentes no ambiente *online*. A NetClean e a Thorn compilaram as melhores práticas para o setor privado no que diz respeito a enfrentar a circulação e a produção de materiais sexuais que envolvem crianças e adolescentes em suas plataformas, além de oferecer suas ferramentas para as empresas detectarem esses materiais [104] [105].

Além de ajudar agências especializadas, dedicadas a promover a segurança *online* de crianças e adolescentes, as empresas também podem fazer uma contribuição significativa para promover o bem-estar digital de crianças e adolescentes ao garantir que, desde seu *design* (*by design*), todos os seus próprios serviços e plataformas estejam seguros (ver página 25 para mais detalhes).

Recomendações 9

Recomendações

O principal objetivo do Grupo de Trabalho da Comissão de Banda Larga sobre Segurança *Online* de Crianças e Adolescentes é conscientizar as pessoas sobre os riscos e as ameaças que existem para crianças e adolescentes no ambiente *online*. Além disso, apresentar uma série de recomendações para minimizar esses riscos e ameaças, e ao mesmo tempo ser capaz de capitalizar os benefícios que a expansão da banda larga proporciona para crianças e adolescentes, principalmente aqueles em países em desenvolvimento.

As recomendações visam a mobilizar a vontade política e a ação coletiva de todos os *stakeholders*, o que inclui governos, regulamentadores, operadoras, setor privado, plataformas de jogos e mídias sociais, prestadores de serviço de internet, ONU, agências com foco em crianças e adolescentes, além dos responsáveis pela Comissão de Banda Larga e seus colegas. Coletivamente, devemos agora priorizar a segurança *online* de crianças e adolescentes.

Atualmente, o mundo digital é o mundo onde a maioria de crianças e adolescentes dos países desenvolvidos vive, se diverte e aprende. Cada vez mais, o mundo digital também está se tornando o mundo de crianças e adolescentes em países em desenvolvimento. Portanto, esse mundo digital deve respeitar o direito das crianças e dos adolescentes de estarem livres de todas as formas de violência, abuso e exploração sexual. Deve se tornar um mundo mais seguro e preparar as futuras gerações para prosperar no espaço digital.

O objetivo dessas recomendações é fornecer uma estrutura que apoie a colaboração e a ação entre os *stakeholders* que desempenham um papel integral em priorizar a segurança *online* de crianças e adolescentes.

Declaração Universal de Segurança *Online* de Crianças e Adolescentes

A Comissão de Banda Larga para o Desenvolvimento Sustentável recomenda que todos os indivíduos e grupos que se consideram defensores dos direitos da criança e do adolescente no espaço digital participem de nossa ação coletiva ao assinar a Declaração Universal de Segurança *Online* de Crianças e Adolescentes para:

Incluir estratégias de segurança *online* de crianças e adolescentes em todos os planos nacionais de banda larga e/ou digitais até 2021

Em 2003, a Comissão de Banda Larga lançou uma iniciativa transformadora envolvendo governos para desenvolver planos de banda larga nacionais. Até o momento, 163 países já implementaram e atualizam esses planos continuamente, com parceiros apoiados pela UIT, que os avalia e os responsabiliza.

Convocamos todos os países a implementarem estratégias baseadas em evidências voltadas para a segurança *online* de crianças e adolescentes, seguindo exemplos como *WeProtect Model National Response* (para o caso de exploração e abuso sexual de crianças e adolescentes e para o caso de materiais sobre abuso sexual de crianças e adolescentes) e outras estratégias que abordam diferentes tipos de ameaças e riscos em seus planos nacionais de banda larga e/ou digitais.

Impedir, detectar, responder e agir

Membros da indústria nacional e internacional, incluindo operadoras, prestadores de serviço de internet e plataformas de jogos e mídias sociais, devem colocar em prática um conjunto de competências mínimas – tecnologias, sistemas e protocolos para detectar e tratar qualquer tipo de abuso (classificado como atividade criminal) contra crianças e adolescentes. Também devem trabalhar com a sociedade civil para conscientizar a população

sobre os problemas relacionados à segurança *online* de crianças e adolescentes e ajudar todos os adultos responsáveis pelo bem-estar de crianças e adolescentes – incluindo pais e responsáveis, escolas, organizações que atuam com crianças e adolescentes e comunidades – a desenvolver o conhecimento e as habilidades necessárias para manter a segurança de crianças e adolescentes.

A definição do trabalho de enfrentamento do abuso *online* contra crianças e adolescentes deve incluir:

- Exploração e abuso sexual de crianças e adolescentes.
- Materiais sobre abuso sexual de crianças e adolescentes.
- Quaisquer outras violações da Convenção sobre os Direitos da Criança das Nações Unidas (UNCRC), incluindo cyber*bullying*, coleta de dados ou prestação de serviços potencialmente prejudiciais para crianças e adolescentes.

Quando os *stakeholders* detectarem algum conteúdo em suas plataformas internas ou em plataformas onde operam, supervisionam como moderadores ou sobre as quais têm algum tipo de responsabilidade, devem reportar e remover esse conteúdo em colaboração com outros atores relevantes.

Líderes da indústria devem auxiliar empresas menores na implementação de soluções tecnológicas, desenvolvimento de capacidades e processos de relato de informação.

Os direitos das crianças e dos adolescentes no que diz respeito à proteção contra crimes (*online* e *offline*) devem ser priorizados sem comprometer o direito à privacidade de todos os usuários da internet (incluindo crianças e adolescentes).

Estabelecer mecanismos claros e controláveis para assegurar que os direitos da criança e do adolescente estejam incluídos no modelo operacional

Crianças e adolescentes já são mais de 30% dos usuários da internet. E a expansão da banda larga nos países em desenvolvimento da África subsaariana, Ásia e América Latina aumentará esse número de maneira significativa.

Reconhecendo esse fato e a particular vulnerabilidade de crianças e adolescentes ao abuso sexual *online*, os *stakeholders* devem se comprometer em instituir uma posição sênior ou uma equipe dedicada a integrar os princípios da Convenção sobre os Direitos da Criança e do Adolescente das Nações Unidas no modelo operacional da organização.

As empresas devem reportar as ações, incluindo resultados, realizadas por essa equipe ou pelo executivo em seus relatórios anuais corporativos e sobre sustentabilidade. Os reguladores e outros órgãos oficiais devem incluir essa informação em sua prestação de contas anual a legisladores ou a outros supervisores.

Padronizar definições e terminologia e desenvolver normas comuns

Os *stakeholders* devem trabalhar em conjunto para desenvolver uma estrutura universal de cooperação na luta contra o abuso sexual *online* de crianças e adolescentes. Isso deve incluir normas para a interoperabilidade legal que permite compartilhamento de dados e inteligência entre setor público, privado e entidades confiáveis da sociedade civil.

Entre os países e os territórios, a legislação deve visar a adoção de definições e terminologia consistentes, bem como a classificação de crimes *online* contra crianças e adolescentes em conformidade com o *WeProtect Model National Response* e outros modelos e estruturas com base em evidências. Quaisquer barreiras legais que possam surgir para empresas que estejam

implementando ferramentas técnicas para combater o abuso de crianças e adolescentes devem ser removidas, incluindo a disponibilização, sem custo para empresas privadas confiáveis, da análise jurídica sobre a segurança *online* de crianças e adolescentes em cada país. Os países devem desenvolver classificação de conteúdo universal para facilitar o compartilhamento de dados.

Dados técnicos devem estar disponíveis entre setores e territórios confiáveis para facilitar os esforços de gerenciamento de casos pelas autoridades legais e auxiliar na identificação da vítima. Os *stakeholders* devem se comprometer a apoiar o trabalho de garantir maior consistência na prática de anotação de *hashes* e entrada de dados. Devem garantir a manutenção segura dos dados relacionados às vítimas identificadas e não identificadas.

Usar *design* apropriado para a idade e consentimento de dados para plataformas de mídias sociais e de jogos, e outros serviços *online* para crianças e adolescentes.

Todas as empresas que desenvolvem ou implementam soluções para proteger crianças e adolescentes, ou materiais que podem ser usados por crianças e adolescentes de alguma forma direta ou indireta, devem minimizar os riscos e as ameaças à sua segurança *online*. Elas devem tomar medidas para verificar a idade, identificar os usuários e impedir qualquer disseminação de ódio, incitação à violência, bem como produção e distribuição de conteúdo *online* prejudicial e ilegal, como os materiais sobre abuso sexual de crianças e adolescentes. As empresas que fornecem produtos, serviços e aplicativos *online* para crianças e adolescentes devem usar um *design* apropriado para a idade, bem com termos e condições adaptados para crianças e adolescentes. Não se deve solicitar a crianças e adolescentes que consintam com algo que não são, na terminologia jurídica, "para o melhor interesse de crianças e adolescentes"

Investir em coleta de dados, pesquisa, bem como em desenvolvimento e expansão de soluções tecnológicas

O setor privado deve trabalhar com outros *stakeholders*, como as ONGs e a academia, para reduzir a abordagem compartimentalizada e fragmentada no desenvolvimento e disponibilidade das ferramentas técnicas (incluindo IA).

A tecnologia que combate as violações *online* dos direitos de crianças e adolescentes deve, sempre que possível, ser aberta ou compartilhada, padronizada, de plataforma agnóstica e colocada à disposição de todos os *stakeholders* relevantes e confiáveis, independente do setor. Os setores privado e público devem investir recursos e apoiar um ao outro no desenvolvimento de soluções tecnológicas para contribuir na luta contra o abuso sexual *online* de crianças e adolescentes.

Esse trabalho não deve prejudicar a aplicação da lei ou da segurança de crianças e adolescentes. Também há a necessidade de investir em pesquisas para entender os impactos das novas tecnologias digitais nas crianças e nos adolescentes para impedir possíveis riscos e perigos, agindo antes que os agressores *online* possam tirar vantagem de novas tecnologias, de lacunas na legislação ou de fenômenos *online* e sociais.

Desenvolver métricas comuns para a segurança *online* de crianças e adolescentes

Ao trabalhar em conjunto, a comunidade internacional deve desenvolver um conjunto universal de métricas para que os *stakeholders* possam medir todos os aspectos relevantes da segurança *online* de crianças e adolescentes. As organizações e os indivíduos podem usar essas métricas para determinar o sucesso de atividades de segurança *online* de crianças e adolescentesao ler os relatórios anuais de instituições e agências, entre outras, como:

- o Banco Mundial e outros bancos de desenvolvimento;
- a Associação da Indústria de Dispositivos Móveis (GSMA)
- a Organização para a Cooperação e Desenvolvimento Econômico (OCDE)
- a União Europeia;
- a União Africana;
- a Liga Árabe;
- o Instituto DQ; e
- o Fórum Econômico Mundial.

O uso das métricas do *The Economist Intelligence Unit Index* e do relatório *Broadband State of the Broadband Commission* ajudará todos os *stakeholders*, entre fronteiras, a acompanhar o progresso nas respostas dos países ao abuso sexual de crianças e adolescentes e outras formas de violência *online*.

Implementar a educação universal em habilidades digitais

Todas as crianças e todos os adolescentes devem ser ensinados sobre habilidades digitais como parte de uma estratégia para minimizar os riscos e maximizar as oportunidades que a tecnologia oferece.

O ensino de habilidades digitais deveria fazer parte do currículo base das escolas e incluir uma educação mais ampla de crianças e adolescentes sobre como lidar com relacionamentos, criar resiliência, desenvolver habilidades de pensamento crítico e buscar ajuda quando precisar.

Para tornar isso possível, recomendamos que os líderes dos setores público, privado e civil implementem, em todos os níveis, o marco de ação de inteligência digital, desenvolvido pelo Instituto DQ (*Digital Quality Institute* – DQI) ou outro equivalente.

Para obter informações complementares, confira o relatório *Technology, Broadband and Education Report:*

https://www.broadbandcommission. org/Documents/publications/BD_ bbcomm-education_2013.pdf

10

Disposições para um modelo de proteção *online* de crianças e adolescentes

Disposições modelo para a proteção *online* de crianças e adolescentes para serem incluídas nos Planos de Banda Larga e Leis contra Crimes Cibernéticos nacionais

Essas disposições visam a servir de modelo para os países usarem ao traçar sua própria seção de proteção *online* de crianças e adolescentes nos seus planos nacionais de banda larga.

1.1 Disposições relevantes que devem ser refletidas nos planos nacionais de banda larga

As seguintes disposições devem ser incluídas nos Planos Nacionais de Banda Larga para estabelecer a base apropriada para uma abordagem fundamentada, efetiva e aplicável à proteção de crianças e adolescentes *online*.

1.1.1 Adesão a convenções e protocolos internacionais

A adesão a convenções e protocolos internacionais demonstra conscientização, disposição e comprometimento de um país em adotar melhores práticas internacionais, códigos de conduta, ferramentas, políticas, terminologias padronizadas e informações compartilhadas, bem como cooperar com outros signatários. Também ajuda a acelerar o conhecimento e a implementação de processos relevantes.

Deve ser incluída uma disposição que estabeleça formalmente a adesão do país à Convenção sobre os Direitos da Criança das Nações Unidas (UNCRC), que entrou em vigor em 2 de setembro de 1990. A UNCRC visa a assegurar uma ampla variedade de direitos humanos para crianças e adolescentes –incluindo direitos civis, culturais, econômicos, políticos e sociais.

Também deve ser incluída uma disposição que define a adesão do país ao Protocolo Facultativo à Convenção sobre os Direitos da Criança Relativo à Venda de Crianças, Prostituição Infantil e Pornografia Infantil das Nações Protocolo Facultativo à Convenção dos Direitos da Criança Relativo à Venda de Crianças, Prostituição Infantil e Pornografia Infantil das Nações Unidas, que entrou em vigor em 18 de janeiro de 2002. Esse é um dos instrumentos jurídicos internacionais mais importantes que pode ser usado para analisar as abordagens legislativas e regulatórias para tratar os crimes de materiais sobre abuso sexual de crianças e adolescentes, em conformidade com as normas internacionais.

Deve ser incluída uma disposição que estabeleça a adesão à Convenção de Budapeste sobre Crimes Cibernéticos, de 23 de novembro de 2001. Essa Convenção representa o primeiro instrumento intergovernamental que trata de crimes com materiais sobre abuso sexual de crianças e adolescentes realizados pelo computador.

Deve ser incluída uma disposição que estabeleça a adesão à Convenção para a Proteção das Crianças contra a Exploração Sexual e os Abusos Sexuais Convenção de Lanzarote sobre a Proteção das Crianças contra a Exploração e os Abusos Sexuais, de 25 de outubro de 2007. Esse instrumento contém disposições que tratam dos crimes de materiais sobre abuso sexual de crianças e adolescentes e crimes de aliciamento *online* (*grooming*). Estabelece as várias formas de abuso sexual de crianças e adolescentes como crimes, incluindo o abuso sexual cometido dentro de casa ou pela família, com o uso de força, coerção ou ameaças.

1.1.2 Definições

Devem ser estabelecidas disposições nos Planos de Banda Larga e nas Leis de Crime Cibernético Nacionais para definir o que significa um crime dentro do contexto de proteção *online* de crianças e adolescentes. Prevê-se que a seguinte definição possa ser adotada:

Um crime contra uma criança ou um adolescente no ambiente *online* deve ser definido como:

- Qualquer ato ou omissão, incluindo, entre outros, a manipulação (produção, preparação, transmissão, armazenamento, publicação ou promoção) de materiais digitais (livros, cartas, desenhos, fotos, filmes, símbolos para fins de exploração, sedução, distribuição ou exibição, gravações de áudio, música, *software*, aplicativos móveis ou jogos eletrônicos), cujo assunto seja referente a menores de 18 anos de idade, e caso o material retrate ou puder ser usado para abuso sexual de menores.

- Aliciamento cibernético (*cyber-grooming*), exploração sexual, contato não autorizado e solicitação de uma criança ou de um adolescente para realizar atos ilegais.

- Fornecimento ilegal a crianças ou adolescentes de bens e/ou serviços destinados a adultos.

- Fornecimento de bens e/ou serviços que, se usados sem restrição, podem fazer com que crianças e adolescentes desenvolvam um vício relacionado à tecnologia que não lhes é saudável.

- Utilização de ferramentas *online* para perpetuar o tráfico de crianças e adolescentes.

- Deixar de denunciar um crime a uma criança ou crianças (ou a um adolescente ou adolescentes), dentro de um prazo razoável, às autoridades policiais ou ao órgão de fiscalização quando um indivíduo ou entidade ficar sabendo do ato real ou intencional de tal crime. Não denunciar um crime contra uma ou mais crianças ou adolescentes, dentro de um período razoável, às autoridades policiais ou órgãos de fiscalização quando um indivíduo ou entidade souber do ato real ou intencional de tal crime.

1.1.3 Iniciativas nacionais

As disposições devem ser descritas nos Planos Nacionais de Banda Larga e estabelecer os compromissos para lançar iniciativas de proteção *online* de crianças e adolescentes baseadas em objetivos específicos.

Por exemplo, o plano de ação adotado pela Suécia:

- Os objetivos do governo são de assegurar que nenhuma criança ou adolescente na Suécia seja sujeita à exploração sexual; que nenhuma criança ou adolescente de outro país seja explorada sexualmente por pessoas da Suécia; que crianças e adolescentes vítimas de exploração sexual recebam todo o apoio e ajuda que precisarem; e que a Suécia contribua para a cooperação internacional eficaz sobre essa questão.

1.1.4 Responsabilidades de intermediários

Deve ser incluída uma disposição que trate das responsabilidades de intermediários, como fornecedores de rede de comunicações eletrônicas e ISPs. A disposição deve demonstrar o compromisso do país para assegurar que empresas de informação, comunicação e tecnologia, que realizam um trabalho dentro das suas fronteiras e atuam como intermediários, tomem medidas concretas para impedir que imagens, vídeos e links para materiais sobre abuso sexual de crianças e adolescentes apareçam em portais gerenciados por essas empresas.

Deve incluir disposições que obriguem os fornecedores de tecnologia a assegurar que novas técnicas de criptografia não impossibilitem o uso de ferramentas desenvolvidas para detectar esse tipo de material, identificar vítimas e colher evidências sobre os agressores.

A lei deverá exigir que os ISPs removam o material de abuso sexual de crianças e adolescentes da visualização pública assim que tomarem ciência deste. Ao mesmo tempo, o ISP deverá denunciar o material e a pessoa ou entidade que o publicou para autoridades legais relevantes ou para centrais de denúncia na internet. Os ISPs não deverão notificar o usuário sobre a remoção do material sobre abuso sexual de crianças e adolescentes, uma vez que correão o risco de alertar os agressores sobre o fato de que estão sob investigação.

1.1.5 Obrigações impostas aos desenvolvedores de jogos

Deve ser incluída uma disposição que exija que os desenvolvedores de plataformas de jogos implementem e disponibilizem controles de tempo de jogo (como padrão – *by default*) e outros controles parentais para monitorar e supervisionar o uso de dispositivos de jogos e minimizar os efeitos adversos de seu uso prolongado e desordenado, resultando em vício. As empresas não envolvidas diretamente no desenvolvimento, mas na comercialização desses jogos *online*, devem empenhar-se para assegurar que os desenvolvedores de plataformas de jogos implementem tais controles. As plataformas de jogos que operam salas de bate-papo, fóruns e outras ferramentas similares devem assegurar que crianças e adolescentes estejam seguros contra aliciamento (*grooming*), *bullying*, roubo de dados e outras ameaças ao utilizarem essas funções.

1.1.6 Compromisso de trabalhar com organismos terceiros

Deve ser incluída uma disposição que comprometa o país a assegurar que ele trabalhe com organizações internacionais, como, por exemplo, ITU *Child Online Protection* (COP), *WeProtect Global Alliance* (WPGAP), *Global Partnership to End Violence Against Children*, *Child Dignity Alliance*, *Virtual Global Taskforce* (VGT) ou *Internet Watch Foundation* (IWF).

O WPGA é um movimento internacional dedicado à ação nacional e à mundial para acabar com a exploração sexual de crianças e adolescentes no ambiente *online*. O VGT é um grupo de colaboração internacional que envolve agências policiais, organizações não governamentais e parceiros do setor privado para proteger crianças e adolescentes da exploração sexual *online* e *offline*. A IWF oferece uma saída segura para qualquer um denunciar de forma anônima imagens e vídeos suspeitos de abuso sexual *online* de crianças e adolescentes, conduz suas buscas usando as melhores tecnologias e remove conteúdo ilegal. Além disso, há outras organizações e iniciativas que tratam de *cyberbullying* ou de outras formas de ameaças e perigos *online*.

1.1.7 Proteção de dados

Deve ser incluída uma disposição na qual o país aplicará a legislação relevante sobre a proteção de dados pessoais e outras medidas de privacidade *online*, voltada principalmente para crianças e adolescentes. O governo do Reino Unido aplicou a Lei de Proteção de Dados em 2018, que inclui disposições sobre proteção de dados específicos para menores de 18 anos e é o líder mundial na utilização de uma abordagem de privacidade padrão (*by default*). A lei se baseia em esforços que proporcionaram à legislação do Reino Unido um melhor entendimento do papel dos dados nas experiências *online* de crianças e adolescentes: por exemplo, o papel dos mecanismos de recomendações por dados em promover material inadequado a usuários com menos de 18 anos, como *sites* pró-anorexia, materiais de automutilação, conteúdo viciante e assim por diante [106]. Atualmente,

muitos outros países estão em processo para seguir esse exemplo.

1.2 Disposições relevantes para as leis contra crimes cibernéticos

1.2.1 Definições

Deve ser incluída uma disposição nas leis contra crimes cibernéticos, definindo o que significa crime cibernético contra crianças e adolescentes. A definição estabelecida acima na seção 1.1.2 se aplica também neste caso.

1.2.2 Estabelecimento de mecanismos de denúncia e agência de apoio institucional para a proteção *online* de crianças e adolescentes

Deve ser incluída uma disposição que estabeleça uma agência oficialmente reconhecida que ofereça apoio institucional para a proteção *online* de crianças e adolescentes. Normalmente, a equipe *Computer Emergency Response Team* (CERT) assume essa responsabilidade de administrar a proteção *online* de crianças e adolescentes, e denuncia ao NCMEC, à Interpol e ao *International Center for Missing & Exploited Children* (ICMEC).

Deve ser incluída outra disposição que institucionalize o estabelecimento de um canal, seja ele um portal, uma central de atendimento ou de denúncia telefônica, uma central de atendimento e denúncia para crianças e adolescentes nacional (quando for viável) ou um aplicativo móvel, por meio do qual os incidentes relacionados à proteção *online* possam ser reportados.

Além disso, deve estar disponível um portal para informar crianças e adolescentes, pais e educadores sobre as ameaças *online*, melhores práticas, políticas e ferramentas para a segurança cibernética, e onde possam ser feitos questionamentos e reclamações.

Da mesma forma, deve ser disponibilizado um portal ao qual representantes do governo, autoridades legais, organizações não governamentais e acadêmicos também possam ter acesso para continuar a monitorar e restringir as ameaças *online*. A Parceria Global pelo Fim da Violência contra Crianças e Adolescentes (*Global Partnership to End Violence Against Children*) com a sua capacidade comprovada de convocação, neutralidade e alcance mundial, poderia exercer um papel importante em criar uma plataforma para que todos os *stakeholders* possam se envolver e agir para tornar crianças e adolescentes seguros no ambiente *online* e estabelecer essa ação dentro de uma agenda mais ampla concentrada em acabar com todas as formas de violência.

Conclusão 11

Conclusão

A humanidade está no meio da 4ª Revolução Industrial conduzida pela conectividade em massa e por tecnologias emergentes como a inteligência artificial (IA), a internet das coisas (IdC), realidade virtual (RV), criptomoedas e a fabricação aditiva (impressão 3D).

A nova revolução industrial, assim como sua predecessora, tem o potencial de nos tornar mais ricos, seguros e felizes. Contudo, da mesma forma que sua predecessora, também traz muitos perigos em potencial, principalmente para crianças e adolescentes.

Entretanto, diferente de nossos antecessores do século XIX, que tinham relativamente pouco controle sobre seu ambiente e apenas uma compreensão parcial sobre as mudanças pelas quais estavam passando, no século XXI, temos a experiência, a tecnologia e os dados para nos ajudar a entender e prever os benefícios e os riscos, além dos perigos associados aos meios pelos quais nossas sociedades estão mudando.

Devemos colocar esse conhecimento e essa expertise em uso a serviço da proteção de nossas crianças e nossos adolescentes contra os perigos no ambiente *online*, bem como contra os perigos no mundo *offline* possibilitados ou promovidos pela atividade *online*. Temos a oportunidade de salvar milhões de crianças e adolescentes de sofrimentos desnecessários, bem como de impedir perigos que tornarão nossas sociedades incapazes de aproveitar o benefício máximo da transformação digital pela qual estão passando.

A boa notícia é que já existem muitas das ferramentas necessárias para agir contra o mal da exploração e do abuso sexual de crianças e adolescentes *online*. Entretanto, com frequência, o trabalho para criá-las em um território não é compartilhado em outra.

Todos os *stakeholders* – governos, autoridades responsáveis pela aplicação da lei, setor privado, especialistas – reconhecem que também precisamos de ferramentas novas e mais efetivas que possam ser compartilhadas, sejam agnósticas com relação a plataforma, de código e/ou acesso aberto.

O setor privado tem boas condições para investir em desenvolvimento e disseminação de soluções tecnológicas em cooperação com governos, ONGs (comunidade especializada), autoridades policiais e outros *stakeholders*. Porém ainda há necessidade de maior apoio, bem como mais financiamento, engajamento e expertise técnica do setor privado. No entanto, ainda há necessidade de promover e fortalecer o apoio às iniciativas globais, como o Fundo pelo Fim da Violência, que, no momento, é a principal iniciativa global que investe no desenvolvimento de soluções tecnológicas.

O tempo e os recursos gastos na duplicação dos esforços poderiam ser usados em detecção e execução ou em alguma outra área de proteção *online* de crianças e adolescentes. Por essa razão, é urgente que os países cooperem para desenvolver normas, sistemas e protocolos comuns. Somente assim, nosso trabalho de proteção de crianças e adolescentes poderá ser tão robusto, eficiente e de rápida ação quanto precisa ser para impedir o flagelo da violência sexual *online* contra crianças e adolescentes, principalmente em países em desenvolvimento, onde a maioria das crianças e adolescentes vive hoje e estará *online* em um futuro próximo.

A exploração e o abuso sexual *online* endêmicos de crianças e adolescentes são evitáveis, mas isso requer que todos nós nos comprometamos em proteger crianças e adolescentes ao acessarem a internet. Devemos trabalhar juntos para empoderar crianças e adolescentes em todos os níveis e estilos de vida para que

possam aproveitar os benefícios da conectividade ao mesmo tempo em que evitam ou minimizam os riscos relacionados que enfrentam na atualidade.

Reconhecemos que ações individuais e coletivas são necessárias para avançar a nossa visão e as nossas metas comuns. Portanto, precisamos:

- Incorporar os direitos da criança e do adolescente na estratégia de banda larga nacional e em todas as outras áreas relevantes da política nacional.
- Cooperar entre fronteiras para criar normas e terminologias válidas em âmbito internacional para definir e medir a situação dos direitos de crianças e adolescentes e da proteção *online*.
- Assegurar que o desenvolvimento de produtos e serviços para crianças e adolescentes pelo setor público, privado ou sociedade civil tenham a garantia dos direitos das crianças e dos adolescentes no centro de seus princípios operacionais.
- Trabalhar com o setor privado, a sociedade civil, especialistas na área e parceiros no desenvolvimento de normas de direitos de crianças e adolescentes no ambiente *online* para nossas respectivas jurisdições.
- Desenvolver meios para engajar os principais *stakeholders* locais em campanhas contra os perigos como a exploração sexual e outros problemas de violação de direitos de crianças e adolescentes no ambiente *online*.
- Usar tecnologias novas e inovadoras como IA, análise e padrões de dados para impedir que redes e serviços sejam usados pelos agressores.
- Realizar progressos mensuráveis no que diz respeito ao bloqueio de *uploads* de materiais sobre abuso sexual, bem como outros materiais não sexuais de violência, que possam prejudicar crianças e adolescentes nos serviços e produtos sob nossos respectivos territórios.
- Fazer com que nossas organizações se comprometam a cooperar além das fronteiras com parceiros relevantes para detectar, cessar e, quando possível, prevenir danos a crianças e adolescentes no ambiente *online*.

Para ajudar a mobilizar todos os que atuam na área de segurança *online* de crianças e adolescentes, o GT desenvolveu a Declaração Universal de Segurança *Online* de Crianças e Adolescentes.

Feita com base nas recomendações do relatório, a declaração é uma expressão de nosso compromisso com crianças e adolescentes e seu bem-estar.

O objetivo da Declaração é ajudar a mobilizar os principais *stakeholders*, como empresas de tecnologia e reguladores que estão na condição de contribuir de maneira direta ou indireta para a melhoraria da segurança *online* de crianças e adolescentes.

Você pode encontrar a Declaração em:

www.childonlinesafety.org

Pedimos, por favor, que compartilhe este relatório com qualquer pessoa que possa ter alguma influência em questões relacionadas à segurança *online* de crianças e adolescentes.

Estudos de caso e melhores práticas

12

Estudo de caso 1: A Convenção sobre os Direitos da Criança das Nações Unidas

Há 30 anos a Convenção sobre os Direitos da Criança das Nações Unidas (UNCRC) tem sido a referência para interpretar os direitos de crianças e adolescentes em diversos ambientes. Seus mais de 40 artigos codificam os direitos das crianças e dos adolescentes e criam uma base pela qual os Estados-nações entendem suas responsabilidades com menores de 18 anos. É o tratado mais ratificado da história, e mais de 190 países são signatários.

Desafio

Em nações com profunda conectividade, crianças e adolescentes têm sido transformados pelo advento e pela adoção de tecnologias que medem, melhoram e interagem com quase todas as experiências de uma criança ou de um adolescente: desde sua educação, suas brincadeiras e seu entretenimento até sua saúde, sua comunicação e justiça. Por outro lado, a falta de conectividade ou acesso à mesma tecnologia, impacta as oportunidades de vida de uma criança ou de um adolescente.

Ao nos concentrarmos em colocar a população mundial *online*, devemos considerar como respeitar os direitos de crianças e adolescentes no ambiente digital; o seu direito de estarem conectados para participar da sociedade, e, uma vez conectados, de manterem e exercerem seus direitos consagrados existentes, a fim de garantir que as tecnologias digitais, desde a concepção de seu *design* (*by design*) e de suas padronizações (*by default*), respeite o desenvolvimento infantil e juvenil.

O Comentário Geral sobre os direitos de crianças e adolescentes em relação ao ambiente digital atua como um complemento à Convenção e estabelece a relevância dos direitos de crianças e adolescentes no mundo digital.

Estratégia

A *5Rights Foundation* apoia o Comitê dos Direitos da Criança (*Committee on the Rights of the Child* – CRC) para desenvolver o Comentário Geral. Liderado pela Professora Sonia Livingstone, o Grupo de Trabalho do Comitê realizou uma minuciosa revisão da literatura, uma consulta pública de três meses, além de *workshops* personalizados com mais de 400 crianças e adolescentes de diferentes contextos em todo o mundo.

Uma consulta com especialistas, realizada pela *5Rights Foundation* em nome do Comitê, ocorrerá em Londres, no outono de 2019. Representando todas as especializações, diferentes setores, nações e contextos, esse grupo especializado conduzirá uma análise detalhada do primeiro rascunho do Comentário Geral. Uma versão revisada irá para avaliação de mais uma consulta pública, que, então, será submetida para aprovação do Comitê, em sua reunião de maio de 2020.

Uma vez formalmente acordado, o Comentário Geral será publicado para um grande grupo de *stakeholders* – e incluíra a publicação do trabalho acadêmico, bem como recursos de interação com crianças e adolescentes, *webinars* e contribuições para eventos sobre políticas, plataformas e mídias.

Resultado

Em um mundo interconectado, se uma criança ou um adolescente não estiver seguro para exercer seus direitos em um determinado contexto, ele ou ela não os exercerá em nenhum outro. O Comentário Geral irá agregar ao nosso conhecimento sobre como desenvolver o mundo digital, levando-se em consideração crianças e adolescentes, e, ao fazer isso, solidificar e proteger seus direitos na era digital.

Estudo de caso 2: Proteção *online* de crianças e adolescentes em Ruanda (financiado pelo *End Violence Fund*)

Com a entrada da banda larga e o aumento na facilidade de compra de *smartphones*, Ruanda decidiu criar uma base que protegesse a segurança *online* de crianças e adolescentes.

Desafio

Ruanda precisava de uma política de segurança *online* de crianças e adolescentes que refletisse as preocupações dos principais *stakeholders* locais, incorporasse as melhores práticas da comunidade global, estivesse de acordo com os processos e as documentações governamentais, e criasse capacidade institucional em uma nova área política.

Foi nesse contexto positivo que o governo de Ruanda convidou a *5Rights Foundation* para desenvolver uma Política de Proteção *Online* de Crianças e Adolescentes. A trabalhar em conjunto com a Professora Julia Davidson da University of East London, a *5Rights Foundation* desenvolveu uma Política Nacional de Proteção *Online* de Crianças e Adolescentes e um Plano de Implementação.

Estratégia

Um grupo multidisciplinar de projeto foi formado no Reino Unido para considerar as principais áreas de políticas. O grupo era composto por especialistas nas áreas de aplicação da lei, violência e trauma em crianças e adolescentes, desenvolvimento infantil, justiça, proteção de dados, telecomunicações, administração, educação, serviços públicos e direitos de crianças e adolescentes.

Áreas semelhantes foram identificadas em Ruanda e, com o apoio do Ministério de Tecnologia, Informação e Inovação de Ruanda, conseguiram envolver colegas profissionais das áreas de justiça, executivo, educação, trabalho social e especialistas em família.

Ao utilizar uma análise abrangente das lacunas – incluindo entrevistas com membros do governo, mesas redondas, revisão literária e *workshops* acadêmicos – a equipe desenvolveu um entendimento sobre a habilidade digital existente em Ruanda.

Todas as questões foram incorporadas na política final e no plano de implementação: os problemas identificados pela análise das lacunas, as questões levantadas pelos tratados sobre políticas, as melhores práticas internacionais existentes e as observações dos membros do grupo de trabalho especializado.

Resultado

A colaboração entre a *5Rights Foundation* e o governo de Ruanda levou à criação de um documento de política alto nível, que define oito objetivos. Esse documento apresentou as principais áreas, as responsabilidades, os facilitadores e o trabalho de múltiplos *stakeholders* que se requer para a proteção *online* de crianças e adolescentes.

Estudo de caso 3: Albânia: internet mais segura e melhor para crianças e adolescentes (financiado pelo *End Violence Fund*)

Geralmente, o domínio ".al" da internet na Albânia, aparece como um dos principais *hosts* de materiais sobre abuso sexual de crianças e adolescentes.

Apesar de a Albânia ter ratificado entre 2016-2018, toda a legislação internacional relevante sobre esse tipo de material, apenas 12 supostos casos de abuso sexual de crianças e adolescentes foram identificados pela polícia e apenas um possível criminoso foi detectado.

Desafio

A análise mostrou que uma estrutura jurídica mal desenvolvida e sem clareza a respeito da proteção de crianças e adolescentes contra os perigos *online* estava contribuindo com as baixas taxas de detecção desses crimes. As convenções internacionais relevantes não são classificadas no direito penal e, como tal, o direito internacional não pode ser acessado ou alavancado.

Estratégia

A Lei sobre Direitos e Proteção de Crianças e Adolescentes da Albânia foi elaborada em 2017 com o suporte técnico do UNICEF. Ela estabelece a garantia da proteção de crianças e adolescentes contra todas as formas de violência, perigo e exploração (*offline* e *online*) e, assim, obriga o governo a implementá-la.

Em seguida, o UNICEF firmou uma sólida plataforma de parceria para que todas as principais instituições governamentais, grupos de sociedade civil, representantes do setor privado, além de crianças e adolescentes, consultem e discutam sobre as disposições de procedimentos concretos para a proteção de crianças e adolescentes contra perigos *online*.

Ao trabalhar com diversos *stakeholders* públicos e privados, a plataforma de parceria criou uma versão final de legislação secundária, que dispõe sobre a implementação da proteção de crianças e adolescentes contra os perigos *online*, que foi elaborada em seis meses e encaminhada com sucesso para a sanção do Conselho de Ministros.

Resultado

Em julho de 2019, o Conselho de Ministros da Albânia aprovou a principal decisão (um regulamento) sobre "Medidas para proteger crianças e adolescentes de materiais *online* prejudiciais e ilegais". Pela primeira vez, é apresentada de forma clara a disposição jurídica e as responsabilidades institucionais para a proteção de crianças e adolescentes contra conteúdo *online* prejudicial e ilegal.

Além disso, estabelece os procedimentos para a remoção imediata de conteúdo da internet que seja prejudicial e ilegal, bem como os canais de denúncia e encaminhamento para violência, *bullying*, exploração e abuso sexual *online* de crianças e adolescentes. O impacto desse resultado de longo alcance afetará de forma positiva quase todas as crianças e os adolescentes da Albânia.

Estudo de caso 4: Filipinas: acabar com a exploração sexual *online* de crianças e adolescentes em Cebu (financiado pelo *End Violence Fund*)

As Filipinas se tornaram um ponto de acesso, e exploração e abuso sexual *online* de crianças e adolescentes está crescendo rapidamente. O governo decidiu então que algo deveria ser feito.

Desafio

Em apenas um mês em 2015, as Filipinas receberam mais de 2.600 encaminhamentos dos Estados Unidos, notificando a detecção de novos *sites* filipinos de abuso sexual de crianças e adolescentes. Até que as leis nas Filipinas

sejam aplicadas de forma mais efetiva, esses números continuarão a subir.

Estratégia

A *International Justice Mission* (IJM), uma ONG de direitos humanos, fez uma parceria com o governo das Filipinas com o intuito de fortalecer a sua capacidade para combater exploração e abuso sexual de crianças e adolescentes no ambiente *online*, em particular a troca de *streamings* ao vivo de abuso sexual infantil e outros materiais de exploração infantil entre os clientes pagantes e os traficantes de crianças e adolescentes.

A IJM trabalhou com o sistema de justiça para resgatar e reabilitar vítimas, bem como responsabilizar agressores pelos crimes, aumentar a capacidade das autoridades locais e diagnosticar lacunas específicas no sistema público de justiça que resultavam em impunidade.

A ONG também fez uma parceria direta com autoridades locais e internacionais – incluindo sistemas da polícia e judiciário – para identificar e resgatar vítimas, prender criminosos e coletar evidências suficientes para sustentar as condenações criminais.

Resultado

Até julho de 2019, a IJM e as autoridades Filipinas trabalharam em conjunto e resgataram 123 crianças e adolescentes de agressores sexuais. Além de resgatar as vítimas, a IJM ajudou a polícia a apreender e acusar 20 criminosos suspeitos e apoiou os promotores a fazerem as acusações contra esses suspeitos, ao mesmo tempo em que apoiou promotores nacionais e locais em casos em andamento.

Além disso, a IJM treinou mais de 50 membros das autoridades responsáveis pela aplicação da lei e 100 juízes e promotores sobre as peculiaridades para investigar e julgar esse tipo de crime. A IJM continua a advogar junto ao Congresso das Filipinas e outras agências para que o governo forneça um compromisso com duração de três anos para fortalecer e treinar os membros da equipe e financiar a Unidade Nacional de Proteção a Crianças, Adolescentes e Mulheres.

Estudo de caso 5: "*I click sensibly*" — educação digital na Polônia

O Escritório de Comunicações Eletrônicas (*Urzad Komunikacji Elektronicznej* – UKE) é o órgão regulador responsável por supervisionar a internet na Polônia, que estava ciente de que muitas crianças e adolescentes, com frequência, utilizavam *smartphones* com pouca ou nenhuma restrição ou orientação.

Desafio

O regulador precisava saber quais tipos de coisa crianças e adolescentes estavam fazendo *online* e quais riscos poderiam estar envolvidos. Além disso, precisava encontrar um meio de educar crianças, adolescentes e pais sobre como estar mais seguros *online* e como entender e gerenciar os riscos.

Estratégia

Em resposta a esses desafios, o UKE criou a campanha *"I click sensibly"* (Eu clico com consciência). A campanha ocorreu em duas partes. A primeira era uma série de aulas sobre a segurança na internet. Durante as aulas, os treinadores do UKE discutiam como navegar *online* de forma responsável, pois deveriam estar atentos ao navegar *online* e como usar os dispositivos de telecomunicação com segurança.

As crianças e adolescentes que participaram dos *workshops* também foram ensinadas sobre como lidar com *cyberbullying*, discursos de ódio,

agressão *online* e como proteger seus dados. As aulas também ensinaram aos pais como filtrar conteúdo inadequado e monitorar crianças e adolescentes sobre como passam seu tempo na internet.

Além disso, o UKE entrevistou um grande número de crianças e adolescentes que participaram das aulas, a fim de descobrir de que maneira usavam a internet e a quais riscos e perigos poderiam estar expostos. Também foram realizadas pesquisas, usando entrevistas pessoais assistidas por computador.

Resultado

Mais de 50 mil crianças e adolescentes se beneficiaram diretamente com as aulas. Com a pesquisa, o UKE também foi capaz de coletar dados detalhados sobre como crianças e adolescentes usavam seu tempo *online*, a quais riscos elas estavam expostos e o quanto seus pais estavam bem equipados para dar suporte a eles.

Em uma época em que muitas agências nacionais e internacionais nem sequer possuem dados sobre a vida *online* de crianças e adolescentes, o UKE possui estatísticas detalhadas sobre essas questões, como, por exemplo, a porcentagem de crianças e adolescentes que foram ridicularizadas ou assediadas *online*, como as crianças e adolescentes são capazes de avaliar a exatidão da informação que encontram na internet e quantos pais exercem controle sobre o que crianças e adolescentes acessam *online*.

Estudo de caso 6: Peru: colaboração intersetorial e interdisciplinar para prevenir e responder à realidade da exploração sexual infantil *online* (financiada pelo *End Violence Fund*)

De acordo com o Instituto de Estatística Nacional, cerca de 50% de crianças e adolescentes entre 6 e 17 anos utilizam a internet no Peru. O Ministro do Interior do país declarou que, entre 2014 e 2017, 22% do tráfego registrado para casos de exploração sexual começaram *online*. Isso ressoa em achados mais amplos do Escritório Internacional de Direitos da Criança advertindo que as tecnologias de informação e comunicação (TIC) têm sido usadas para aliciar crianças e adolescentes *online* para então traficá-las para exploração sexual.

Desafio

O Peru já possui uma política e uma estrutura jurídica relativamente robusta para enfrentar a exploração sexual de crianças e adolescentes em comparação a outros países da América Latina.

O país assinou pactos como ODS, CRC, WPGA *Model National Response Statement of Action* e à Convenção de Budapeste sobre Crime Cibernético. Entretanto, é baixo o número de denúncias e casos que chegam ao tribunal. Além disso, nenhuma dessas políticas ou marcos jurídicos menciona de maneira explicita como abordar e lidar com essa crescente questão de exploração e abuso sexual de crianças e adolescentes *online*. Também há imensas lacunas entre as informações sobre essa questão, as novas formas de

exploração sexual *online*, os recursos e os mecanismos para proteger crianças e adolescentes, além de coordenação entre os setores, treinamento e conscientização.

Estratégia

Com o apoio financeiro do *End Violence Fund* e *Capital Humano y Social Alternativo* (CHS) – uma organização não governamental de direitos humanos com sede no Peru – o país desenvolveu mudanças no Código Penal peruano que expandiram a definição de exploração e abuso sexual de crianças e adolescentes e criminalizou essa atividade em cada contexto. A contribuição mais importante do CHS foi o suporte técnico fornecido à Comissão de Mulheres e Família e à Comissão de Justiça e Direitos Humanos do Congresso da República.

Graças ao CHS e aos esforços das organizações de apoio, 10 artigos do Código Penal serão modificados e outros sete serão adicionados. As alterações propostas criam crimes e sentenças específicos relativos à exploração sexual de crianças e adolescentes, como o recebimento de benefício decorrente de exploração sexual de crianças e adolescentes, bem como coordenação, promoção ou favorecimento desta prática. Pagar para ter relações com crianças ou adolescentes também está contemplado como crime pelo Código Penal revisado.

Além de trabalhar para essa mudança sistêmica, o CHS também chamou a atenção para essa ameaça e educou quase 400 crianças e adolescentes e 600 membros da comunidade (professores, pais e prestadores de serviço) sobre como responder à exploração sexual de crianças e adolescentes, engajando as principais mídias e oferecendo treinamento presencial.

Resultado

O Congresso aprovou o projeto e a versão final foi assinada pelo Presidente do Peru em junho de 2019.

Estudo de caso 7: Proteção *online* de crianças e adolescentes no Vietnã (financiado pelo *End Violence Fund*)

Assim como aumentou o número de crianças e adolescentes *online* no Vietnã, aumentaram também os riscos. Para enfrentar essa questão de segurança *online*, o ChildFund Vietnam criou a iniciativa Swipe Safe.

Desafio

Em 2018, os jovens entre 15 e 24 anos contabilizaram mais de um terço dos 54,7 milhões de internautas no Vietnã. Isso aumentou sua exposição a todas as formas de abuso sexual, de outros perigos *online*, chegando ao ponto em que um em cada três estudantes no país sofriam *cyberbullying*.

Essa questão é ainda mais exacerbada pelos baixos níveis de alfabetização digital de crianças e adolescentes e de seus pais. Com a falta de ferramentas e materiais que promovam a segurança *online*, há pouca compreensão sobre o comportamento *online* de risco e pouca ou nenhuma orientação sobre como se manter seguro *online*.

Estratégia

Para ajudar crianças e adolescentes a navegar na internet com segurança, o ChildFund Vietnam estabeleceu a iniciativa Swipe Safe. Esse programa ensina sobre os possíveis riscos *online*, como *cyberscams*, *bullying* ou abuso sexual e oferece orientação sobre os métodos para se manter seguro.

O programa Swipe Safe incentiva pais, crianças e adolescentes, bem como escolas e o setor privado a exercer um papel ativo na segurança *online* de crianças e adolescentes. Oferece

treinamento para pais e gerentes de *cyber* cafés para identificar e tratar os riscos para crianças e adolescentes. Também ajuda escolas a desenvolverem políticas de fácil entendimento para crianças e adolescentes e orientação sobre segurança *online*.

Uma das principais inovações do programa é o envolvimento de voluntários jovens com vasto conhecimento de tecnologia para treinar outros em suas comunidades locais. Esses treinadores se relacionam diretamente com as experiências de outros jovens e mantêm o currículo atualizado.

Resultado

Até junho de 2019, mais de 8.700 adolescentes, 1.100 pais e 100 "parceiros de segurança *online*" (incluindo oficiais do governo, representantes de escolas e membros da União Jovem) receberam treinamento em segurança *online* por meio do programa.

Pesquisas indicaram que 91% de crianças e adolescentes que participaram do estudo demonstraram maior conhecimento em segurança *online*. Isso incluiu habilidades como configurações de privacidade, verificações de informações, compartilhamento responsável, pesquisas *online* e denúncia de conteúdo prejudicial. Entre os pesquisados, 89% sabiam para onde se dirigir para obter suporte e 30% se sentiam mais seguros *online*.

Estudo de Caso 8: Utilizar a tecnologia para manter crianças e adolescentes seguros: trabalho do Facebook com o NCMEC

Desafio

O abuso sexual de crianças e adolescentes é um crime que afeta uma estimativa de 9 a 19,7% de meninas e 3 a 7,9% de meninos. Especialistas em segurança, ONGs, governos e empresas possuem interesse em romper e impedir a exploração sexual de crianças e adolescentes nas tecnologias *online* e precisam trabalhar em conjunto quando possível para serem mais efetivos.

Estratégia

Sendo o órgão centralizador nos Estados Unidos e o centro abrangente de denúncias para todas as questões relacionadas à prevenção e à recuperação de crianças e adolescentes vítimas, o NCMEC lidera a luta contra sequestro, abuso e exploração sexual.

Desde 2016, o Facebook sedia uma maratona de *hackers* entre as diversas indústrias de tecnologia, a *Hackathon* Anual de Segurança de Crianças e Adolescentes (*Child Safety Hackathon*), para desenvolver novas ferramentas e tecnologias em segurança de crianças e adolescentes, sem fins lucrativos, para parceiros como o NCMEC. O evento de dois dias reúne engenheiros e cientistas de dados das empresas parceiras da Coalização Tecnológica e outros para desenvolver novas tecnologias que ajudam a proteger crianças e adolescentes. As *Hackathon*s anuais são uma forma interessante de reunir pessoas de diferentes organizações com uma vasta gama de conhecimento para construir ferramentas que enfrentam problemas como a exploração e abuso

sexual *online* de crianças e adolescentes. Todos os códigos abertos e protótipos desenvolvidos na *Hackathon* de Segurança de Crianças e Adolescentes são doados para a Coalizão Tecnológica e seus parceiros de segurança, como o NCMEC, para serem usados em seus esforços de segurança de crianças e adolescentes.

Com base na generosa contribuição de dez anos atrás pela Microsoft do PhotoDNA para lutar contra a exploração sexual; e, mais recentemente, no lançamento do Google Content Safety API, o Facebook também anunciou na *Hackathon* de 2019 que está disponibilizando em código aberto duas tecnologias que detectam fotos e vídeos idênticos e quase idênticos – compartilhando parte da tecnologia que usam para enfrentar abusos em sua plataforma com outros que também estão trabalhando para manter a internet segura. Esses algoritmos têm o código aberto no GitHub para que parceiros do setor privado, pequenos desenvolvedores e organizações sem fins lucrativos possam usá-los para identificar com mais facilidade conteúdos abusivos e compartilhar *hashes* – ou impressões digitais – de diferentes tipos de conteúdo prejudicial. Para aqueles que já utilizam sua própria tecnologia de equiparação de conteúdo ou outra semelhante, essas tecnologias são uma outra camada de defesa e permitem que sistemas de compartilhamento de *hash* conversem entre si, tornando os sistemas muito mais poderosos.

Resultados

Entre os protótipos desenvolvidos na *Hackathon* estão projetos que melhoram a eficiência do trabalho das pessoas que identificam e resgatam crianças e adolescentes, tornando mais fácil classificar com rapidez as imagens e os dados, além de priorizar os casos. Por exemplo, em 2019, as equipes desenvolveram um protótipo de função que permitirá a ferramenta CiberTipline de gerenciamento de caso do NCMEC consultar e comparar pontos dentro de banco de dados de outras organizações sem fins lucrativos em busca de *hashes* conhecidos e outras informações essenciais. Isso ajudará a identificar crianças e adolescentes em risco e destacar as denúncias mais importantes. O protótipo vencedor de 2018, chamado *SpottingTrends*, utiliza análise de *clustering* e informações que estão associadas a exploradores sexuais de crianças e adolescentes conhecidos para ajudar a assegurar que esses indivíduos não sejam capazes de navegar em outro lugar na internet. E o sucesso da aplicação no mundo real do protótipo que vencedor de 2016 – um mecanismo de busca de crianças e adolescentes que procura a correspondência entre fotos *online* com as disponíveis no banco de dados do NCMEC de crianças e adolescentes desaparecidas – confirmam o benefício de utilizar tecnologia para ajudar a enfrentar essas questões desafiadoras. Tecnologias desse tipo têm o potencial de reduzir o tempo de resposta das autoridades responsáveis pela aplicação da lei, levando ajuda de forma mais rápida e eficiente a crianças e adolescentes que podem estar vulneráveis.

Glossário 13

Glossário

Aliciamento – *Grooming* – O processo pelo qual um adulto cria uma relação com uma criança/adolescente para facilitar o contato *online* ou *offline* para fins que irão prejudicar a criança/adolescente (por exemplo, radicalização ou abuso sexual).

Aliciamento cibernético – *Cyber grooming* – O processo de "fazer amizade" com uma criança ou um adolescente online para incentivar contato sexual *online* e/ou um encontro presencial com o objetivo de cometer abuso sexual [108].

Bullying – Um tipo de violência cometido por um padrão de comportamento indesejado e agressivo que envolve um desequilíbrio de poder real ou percebido, e exerce um impacto negativo na vítima, no agressor e nas testemunhas. O comportamento é repetido ou tem o potencial para ser repetido ao longo do tempo [109].

***Bullying* cibernético** – *cyberbullying* ou *bullying* feito por meio de canais eletrônicos, como *chats*, mídias sociais, e-mail e SMS.

By default – Desde a configuração padrão de um *software*, por exemplo, o tamanho ou o estilo da fonte [110].

By design – Desde a fase de *design* de um *software*; ou seja, desde sua modelagem, organização e estruturação [111].

CAM – *Child abuse material* – Material sobre abuso infantil.

CHS – *Capital Humano y Social Alternativo*.

COP – *Child Online Protection* – Segurança online de crianças e adolescentes.

COPPA – *The US Child Online Privacy Protection Act* – Lei de Proteção à Privacidade Online da Criança dos EUA.

CRBP – *Children's Rights and Business Principles* – Direitos de Crianças e Adolescentes e Princípios de Negócios.

CRC – *Committee on the Rights of the Child* – Comitê dos Direitos da Criança.

CSAM – *Child Sexual Abuse Material* – Materiais sobre abuso sexual de crianças e adolescentes.

CSEA – *Child Sexual Exploitation and Abuse* – Exploração e abuso sexual de crianças e adolescentes.

Darknet – *Sites* e serviços que são criptografados para impedir que usuários ou publicadores sejam rastreados.

Deepfake – Uma simulação de foto ou vídeo bastante realista que parece uma pessoa real.

DQI – *Data Quality Institutes* – Institutos com qualidade de dados.

ECPAT – *End Child Prostitution and Trafficking* – Fim da Prostituição e do Tráfico de Crianças e Adolescentes.

EIU – *The Economist Intelligence Unit* – Unidade de Inteligência da revista *The Economist*.

GSA – *Global Cybersecurity Agenda* – Agenda Global de Segurança Cibernética.

GSMA – *Global Mobile Industry Association* – Associação da indústria de Dispositivos Móveis.

GT – Grupo de Trabalho.

Hashing – Uma tecnologia que cria uma assinatura única para um arquivo digital, usada na detecção automática de CSAM.

Hackathon – Maratona de *hackers*.

IA – Inteligência artificial.

ICCAM – Uma plataforma segura usada para coletar, trocar e classificar denúncias de materiais sobre abuso sexual que suporta a rápida remoção de conteúdo da internet (INHOPE).

IdC – Internet das coisas.

IJM – *International Justice Mission* – Missão de Justiça Internacional.

INHOPE – *International Association of Internet Hotlines* – Associação Internacional de Canais de Denúncia.

Interpol – *International Police* – Polícia Internacional.

ISIS – Grupo *jihadista* do Estado Islâmico.

ISPs – *Internet service providers* – Prestadores de serviço de internet.

IWF – *Internet Watch Foundation* – Fundação de Observação da Internet.

LEA – Agência/Autoridade de Manutenção da Ordem Pública.

NCMEC – *National Center for Missing & Exploited Children* – Centro Nacional de Crianças e Adolescentes Perdidas e Exploradas.

NSPCC – *National Society for the Prevention of Cruelty against Children* – Sociedade Nacional para a Prevenção da Crueldade contra Crianças do Reino Unido.

OCDE – *Organisation for Economic Co-operation and Development* – Organização para a Cooperação e Desenvolvimento Econômico

ODS – Objetivos de Desenvolvimento Sustentável.

OMS – *World Health Organization* – Organização Mundial da Saúde.

ONG – Organizações não governamentais.

ONU – *United Nations Organization* – Organização das Nações Unidas.

P2P – *Peer-to-peer file sharing services* – Serviços de compartilhamento de arquivo de pares para pares.

PIB – Produto Interno Bruto.

RV – Realidade virtual.

Stakeholders – Partes Interessadas.

Sexting – Divulgação de conteúdos eróticos e sensuais através de celulares.

UIT – *International Telecommunications Union* – União Internacional de Telecomunicações.

UKE – *Urzad Komunikacji Elektronicznej* – Escritório de Comunicações Eletrônicas.

UNCRC – *United Nations Convention on the Rights of the Child* – Convenção sobre os Direitos da Criança das Nações Unidas.

UNICEF – *United Nations Children's Fund* – Fundo das Nações Unidas para a Infância.

VPNs – *Virtual Private Networks* – Redes Privadas Virtuais.

Web Crawlers – Rastreadores de web.

WPGA – *WeProtect Global Alliance* – Aliança Global NósProtegemos.

Referências 14

Referências

1. UNICEF DATA. *The State of the World's Children 2017 Statistical Tables.* 2019. Disponível em: https://data.unicef.org/resources/state-worlds-children-2017-statistical-tables/. Acesso em: 5 ago. 2019.

2. Loritz, M. *UK-based Cyan Forensics partners with major US nonprofit to stop child sexual abuse*. EU-Startups, 2019. Disponível em: https://www.eu-startups.com/2019/08/uk-based-cyan-forensics-partners-with-major-us-nonprofit-to-stop-child-sexual-abuse/. Acesso em: 25 ago. 2019.

3. Comparitech. *Cyberbullying Statistics and Facts for 2016-2019*. Comparitech, 2019. Disponível em: https://www.comparitech.com/internet-providers/cyberbullying-statistics/. Acesso em: 8 ago. 2019.

4. Dqinstitute.org. *Outsmart Cyber-Pandemic*. 2019. Disponível em: https://www.dqinstitute.org/2018DQ_Impact_Report/. Acesso em: 6 set. 2019.

5. Madigan, Sheri et al. The Prevalence of unwanted online sexual exposure and solicitation among youth: a meta-analysis. *Journal of Adolescent Health*, v. 63, n. 2, p. 133-141, 2019.

6. Benoliel, Uri; Becher, Shmuel I. *The Duty to read the unreadable*. Boston College Law Review, n. 60, 11 Jan. 2019. Disponível em: https://ssrn.com/abstract=3313 837 ou http://dx.doi.org/10.2139/ssrn.3313837.

7. Lu, J. Here's how every country ranks when it comes to child abuse and child safety. *UN Dispatch*, 2019. Disponível em: https://www.undispatch.com/here-is-how-every-country-ranks-on-child-safety/. Acesso em: 8 ago. 2019.

8. UNICEF. *Generation unlimited*: business plan for digital connectivity. New York, 2019.

9. ITU. Press Release. *ITU releases 2018 global and regional ICT estimates*. Geneva, 07 Dec. 2018. Disponível em: https://www.itu.int/en/mediacentre/Pages/2018-PR40.aspx. Acesso em: 3 ago. 2019.

10. Provider, S.; Forecasts, V.; Papers, W. Cisco visual networking index: forecast and trends, 2017-2022. *Cisco White Paper*, 2019. Disponível em: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html. Acesso em: 3 ago. 2019.

11. Katoa 'Utoikamanu, F.; Sanou, B. *CTs, LDCs and the SDGs achieving universal and affordable internet in the least developed countries*. Unohrlls.org. 2019. Disponível em: http://unohrlls. org/custom-content/uploads/2018/01/D-LDC-ICTLDC-2018-PDF-E.pdf. Acesso em: 3 ago. 2019.

12. World Bank. *Gains in financial inclusion, gains for a sustainable world*. Washington, DC, 2019. Disponível em: https://www.worldbank.org/en/news/immersive-story/2018/05/18/gains-in-financial-inclusion-gains-for-a-sustainable-world. Acesso em: 3 ago. 2019.

13. UNESCO-UIS. *Sudan*: education and literacy. 2019. Disponível em: http://uis.unesco.org/en/country/sd?theme=education-and-literacy. Acesso em: 3 ago. 2019.

14. 5Rights Foundation. *The Internet on our own terms*. 2019. Disponível em: https://5rightsfoundation.com/static/Internet-On-Our-Own-Terms.pdf. Acesso em: 6 set. 2019.

15. IWF. *Once upon a year*: the Internet Watch Foundation annual report 2018. United Kingdom, 2019. Disponível em: https://www.iwf.org.uk/sites/default/files/reports/2019-04/Once%20upon%20a%20year%20-%20IWF%20Annual%20Report%202018.pdf. Acesso em: 5 ago. 2019.

16. Reyes, I.; Wijesekera, P.; Reardon, J.; Elazari Bar On, A.; Razaghpanah, A.; Vallina-Rodriguez, N.; Egelman, S. *Won't somebody think of the children?*: examining COPPA compliance at scale. Petsymposium.org, 2019. Disponível em: https://petsymposium.org/2018/files/papers/issue3/popets-2018-0021.pdf. Acesso em: 5 ago. 2019.

17. Patchin, J. *2016 Cyberbullying Data*. Cyberbullying Research Center, 2019. Disponível em: https://cyberbullying.org/2019-cyberbullying-data. Acesso em: 5 ago. 2019.

18. Atchoarena, D.; Selwyn, N.; Chakroun, B.; Fengchun, M. *Working Group on Education*: digital skills for life and work. UNESCO, Sep. 2017. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000259013. Acesso em: 6 set. 2019.

19. World Economic Forum. *Cyber-risk exposure among 8-12-year olds drops by 15%*. 2019. Disponível em: https://www.weforum.org/our-impact/helping-young-people-safely-navigate-the-digital-world. Acesso em: 6 ago. 2019.

20. Byrne, J.; Burton, P. *Children as Internet users*: how can evidence better inform policy debate? Taylor & Francis, 2019. Disponível em: https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1291698?hootPostID=1753d7ca474ab7a748bcee5f22ffe65e. Acesso em: 7 ago. 2019.

21. Mascheroni, G.; Ólafsson, K. Access and use, risks and opportunities of the internet for Italian children. *Global Kids Online*, 2019. Disponível em: http://globalkidsonline.net/wp-content/uploads/2017/10/Executive-summary-Italy-june-2018.pdf. Acesso em: 7 ago. 2019.

22. Global Kids Online. *Global Kids Online Serbia*: balancing between opportunities and risks: results from the pilot study. 2019. Disponível em: http://globalkidsonline.net/wp-content/uploads/2016/05/Country-report_Serbia-final-26-Oct-2016.pdf. Acesso em: 7 ago. 2019.

23. 5Rights Foundation. *Towards an internet safety strategy*. 2019. Disponível em: https://5rightsfoundation.com/static/5rights_Towards_an_Internet_Safety_Strategy_FINAL.pdf. Acesso em: 6 set. 2019.

24. ICO. *Age appropriate design*: a code of practice for online services. United Kingdom, 2019. Disponível em: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/age-appropriate-design-a-code-of-practice-for-online-services. Acesso em: 6 set. 2019.

25. Office of the eSafety Commissioner. *Safety by design*. 2019. Disponível em: https://www. esafety.gov.au/esafety-information/safety-by-design. Acesso em: 6 set. 2019.

26. Courtland, R. *Bias detectives*: the researchers striving to make algorithms fair. Nature.com, 2019. Disponível em: https://www.nature.com/articles/d41586-018-05469-3. Acesso em: 8 Aug. 2019.

27. Przybylski, Andrew K.; Nash, Victoria. *Cyberpsychology, behavior, and social networking*. Jul. 2018. DOI: http://doi.org/10.1089/cyber.2017.0466.

28. UNICEF. *The State of the world's children 2017*: children in a digital world. New York, 2019. Disponível em: https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf. Acesso em: 8 ago. 2019].

29. ITU. *ICT facts and figures 2017*. Geneva, 2019. Disponível em: https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx. Acesso em: 8 ago. 2019.

30. UNICEF. *The State of the world's children 2017*: children in a digital world. New York, 2018. Disponível em: https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf. Acesso em: 8 ago. 2019.

31. Africanews. Digital in 2018: Africa's internet users increase by 20%. *Africanews*, 2019. Disponível em: https://www.africanews.com/2018/02/06/digital-in-2018-africa-s-internet-users-increase-by-20-percent/. Acesso em: 8 ago. 2019.

32. Quartz Africa. *Gender inequality in tech starts with teenagers on their cell phones*. 2019. Disponível em: https://qz.com/africa/1420938/girls-have-less-access-to-mobile-phones-than-boys-study-shows/. Acesso em: 25 ago. 2019.

33. IWF. *Exposing child victims*: the catastrophic impact of DNS-over-HTTPs. United Kingdom, 2019. Disponível em: https://www.iwf.org.uk/news/exposing-child-victims-catastrophic-impact-of-dns-over-https. Acesso em: 7 set. 2019.

34. Fox News. *Hany Farid:* Facebook's plan for end-to-end encryption sacrifices a lot of security for just a little bit of privacy. 2019. Disponível em: https://www.foxnews.com/opinion/hany-farid-facebook-end-to-end-encryption-security-privacy. Acesso em: 7 set. 2019.

35. Interpol. *International Child Sexual Exploitation database*. London, 2019. Disponível em: https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database. Acesso em: 8 ago. 2019.

36. Thorn. *The Intersection of Technology and Child Sexual Abuse*. 2019. Disponível em: https://www.thorn.org/child-sexual-exploitation-and-technology/. Acesso em: 8 ago. 2019.

37. Puddephatt, A.; Hargreaves, S. *2018 Annual Report*. United Kingdom: IWF, 2019. Disponível em: https://www.iwf.org.uk/report/2018-annual-report. Acesso em: 8 ago. 2019.

38. Canadian Centre for Child Protection. *Resources & research*: international survivors' survey. Canada, 2019. Disponível em: https://protectchildren.ca/en/resources-research/survivors-survey-results/. Acesso em: 25 ago. 2019.

39. Ecpat. *Towards a global indicator on unidentified victims in child sexual exploitation material*. 2019. Disponível em: https://www.ecpat.org/wp-content/uploads/2018/03/TOWARDS-A-GLOBAL-INDICATOR-ON-UNIDENTIFIED-VICTIMS-IN-CHILD-SEXUAL-EXPLOITATION-MATERIAL-Summary-Report.pdf. Acesso em: 6 set. 2019.

40. NetClean. *The NetClean report 2018*. 2019. Disponível em: https://www.netclean. com/netclean-report-2018/. Acesso em: 12 ago. 2019.

41. Young, Rachel; Tully, Melissa. Nobody wants the parents involved: social norms inparent and adolescent responses to cyberbullying. *Journal of Youth Studies*, v. 22, n. 6, p. 856-872. DOI: 10.1080/13676261.2018.1546838.

42. Childnet. *Young people's experiences of online sexual harassment*: a cross-country report from Project Deshame. 2019. Disponível em: https://www.childnet.com/ufiles/Project_ deSHAME_ Dec_2017_Report.pdf. Acesso em: 8 ago. 2019.

43. Icmec. *Online grooming of children for sexual purposes*: model legislation & global review. 2019. Disponível em: https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf. Acesso em: 8 ago. 2019.

44.Teliacompany. *Children and online privacy*: findings from the children's advisory panel 2017/18. 2019. Disponível em: https://www.teliacompany.com/globalassets/telia-company/documents/sustainability/children-and-online-privacy.pdf. Acesso em: 12 ago. 2019.

45. Brumfield, B. *3 girls skipped school to sneak off and join ISIS*. CNN, 2019. Disponível em: https://edition.cnn.com/2014/10/22/us/colorado-teens-syria-odyssey/index.html. Acesso em: 8 ago. 2019.

46. Martelozzo, E. *A quantitative and qualitative examination of the impact of online pornography on the values, attitudes, belief sand behaviours of children and young people*. United Kingdom: Mdx, 2019. Disponível em: https://www.mdx.ac.uk/__data/assets/pdf_file/0021/223266/MDX-NSPCC-OCC-pornography-report.pdf. Acesso em: 9 ago. 2019.

47. ITV News. *Children report feeling unprotected from inappropriate content on social media sites*. 2019. Disponível em: https://www.itv.com/news/utv/2017-04-27/children-warn-social-media-sites-are-failing-to-shield-them-from-inappropriate-and-dangerous-content/. Acesso em: 9 ago. 2019.

48. Shieber, J. 2018 really was more of a dumpster fire for online hate and harassment: ADL study finds. *TechCrunch*, 2019. Disponível em: https://techcrunch.com/2019/02/13/2018-really-was-more-of-a-dumpster-fire-for-online-hate-and-harassment-adl-study-finds/. Acesso em: 9 ago. 2019.

49. Kardefelt-Winther, D. *Child rights and online gaming*: opportunities & challenges for children and the industry. ECPAT International, 2019. Acesso em: 9 set. 2019.

50.Fitzpatrick, C. Watching violence on screens makes children more emotionally distressed. *The Conversation*, 19 Nov. 2018. Disponível em: https://theconversation.com/watching-violence-on-screens-makes-children-more-emotionally-distressed-106757. Acesso em: 9 ago. 2019.

51. Livingstone, S.; Kirwil, L.; Ponte, C.; Staksrud, E. *In their own words*: what bothers children online? United Kingdom: LSE, 2019. Disponível em: https://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/Intheirownwords020213.pdf. Acesso em: 9 ago. 2019.

52. Calado, F.; Alexandre, J.; Griffiths, M. D. *Prevalence of adolescent problem gambling*: a systematic review of recent research. J Gambl Stud, n. 33, p. 397, 2017. DOI: https://doi.org/10.1007/s10899-016-9627-5.

53. Valentine, G. *Children and young people's gambling: research review*; report by Professor Gill Valentine for the Responsible Gambling Trust. About.gambleaware.org, 2019. Disponível em: https://about.gambleaware.org/media/1274/1-june-update-children-young-people-literature-review.pdf. Acesso em: 9 ago. 2019.

54. Karlsson, Anna; Hakansson, Anders. Gambling disorder, increased mortality, suicidality, and associated comorbidity: a longitudinal nationwide register study. *Journal of Behavioral Addictions*, n. 7, p.1-9, 2018. DOI: 7.1-9. 10.1556/2006.7.2018.112.55.

55. Howard, J. *What's the age when kids start social media?* CNN, 2019. Disponível em: https://edition.cnn.com/2018/06/22/health/social-media-for-kids-parent-curve/index.html. Acesso em: 9 ago. 2019.

56. BBC News. *Under-age social media use 'on the rise'*. 2019. Disponível em: https://www.bbc. co.uk/news/technology-42153694. Acesso em: 9 ago. 2019.

57. United Kingdom. Parliament. *Impact of social media and screen-use on young people's health*. London, 2019. Disponível em: https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/822/822.pdf. Acesso em: 9 ago. 2019.

58. Power, Sally; Taylor, Chris; Horton, Kim. Sleepless in school? The social dimensions of young people's bedtime rest and routines. *Journal of Youth Studies*, v. 20, n. 8, p. 945-958, 2017. DOI:10.1080/13676261.2016.1273522.

59.Cramer, S.; Inkster, B. *#Status Of Mind*: social media and young people's mental health and wellbeing. United Kingdom: Rsph, 2019. Disponível em: https://www.rsph.org.uk/uploads/assets/uploaded/d125b27c-0b62-41c5-a2c0155a8887cd01.pdf. Acesso em: 9 ago. 2019.

60. Meyer, Marisa; Adkins, Victoria; Yuan, Nalingna; Weeks, Heidi M.; Yung-Ju, Chang; Radesky, Jenny. Advertising in young children's Apps. *Journal of Developmental & Behavioral Pediatrics*, n. 1, 2018.

61. Binns, Reuben; Lyngs, Ulrik; Van Kleek, Max; Zhao, Jun; Libert, Timothy; Shadbolt, Nigel. Third party tracking in the mobile ecosystem. *SocArXiv Papers*, 02, Jul. 2018. DOI: 10.31235/osf.io/u7qmz.

62. Todorovic, N.; Chaudhuri, A. *Using AI to help organizations detect and report child sexual abuse material online.* Google, 2019. Disponível em: https://www.blog.google/around-the-globe/google-europe/using-ai-help-organizations-detect-and-report-child-sexual-abuse-material-online/. Acesso em: 10 ago. 2019.

63. Richter, I. *Automatische Bilderkennung hilft im Einsatz gegen Kinderpornografie*. Deutschland: News Center Microsoft, 2019. Disponível em: https://news.microsoft. com/de-de/ki-im-einsatz-gegen-kinderpornografie/. Acesso em: 10 ago. 2019.

64. Vleugels, A. AI-algorithms identify pedophiles for the police: here's how it works. *The Next Police*, 2019. Disponível em: https://thenextweb.com/the-next-police/2018/11/08/ai-algorithms-identify-sexual-child-abuse-for-the-police/. Acesso em: 10 ago. 2019.

65. Griffeye. *Griffeye releases new AI technology trained to aid child abuse investigations*. 2019. Disponível em: https://www.griffeye.com/griffeye-releases-new-ai-technology-press/. Acesso em: 10 ago. 2019.

66. Burgess, M. *AI is helping UK police tackle child abuse way quicker than before*. United Kindgom: Wired, 2019. Disponível em: https://www.wired.co.uk/article/uk-police-child-abuse-images-ai. Acesso em: 10 ago. 2019.

67. Griffeye. *New AI technology trained to aid child abuse investigations*. 2019. Disponível em: https://www.griffeye.com/new-ai-technology-trained-to-aid-child-abuse-investigations/. Acesso em: 6 set. 2019.

68. Ward, M.; Balian, S. Combating online radicalisation with expanded AI capabilities. *Faculty*, 2019. Disponível em: https://faculty.ai/blog/combating-online-radicalisation-with-expanded-ai-capabilities/. Acesso em: 10 ago. 2019.

69. Boyce, J. Facebook touts use of artificial intelligence to fight child exploitation. *NBC News*, 2019. Disponível em: https://www.nbcnews.com/tech/tech-news/facebook-touts-use-artificial-intelligence-fight-child-exploitation-n923906. Acesso em: 10 ago. 2019.

70. United Kingdom. Parliament. *Impact of social media and screen-use on young people's health*: government response to the Committee's Fourteenth Report - Science and Technology Committee - House of Commons. 2019. Disponível em: https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/2120/212002.htm. Acesso em: 25 ago. 2019].

71. Marinus Analytics. Disponível em: https://www.marinusanalytics.com.

72. Computer Weekly. *Thorn CEO on using machine learning and tech partnerships to tackle online child sex abuse*. 2019. Disponível em: https://www.computerweekly.com/news/450415609/Thorn-CEO-on-using-machine-learning-and-tech-partnerships-to-tackle-online-child-sex-abuse. Acesso em: 6 set. 2019.

73. Minton, L. What is human trafficking, and how can technology combat it? *ASU Now*: Access, Excellence, Impact, 2019. Disponível em: https://asunow.asu.edu/20190313-what-human-trafficking-and-how-can-technology-combat-it. Acesso em: 10 Aug. 2019.

74. Phys. *Instagram rolls out new features to counter bullying with AI*. 2019. Disponível em: https://phys.org/news/2019-07-instagram-features-counter-bullying-ai.html. Acesso em: 10 ago. 2019.

75. Eropean Union. *CREEP Project*: cyberbullying effects prevention. Disponível em: http://creep-project.eu.

76. Simonite, T.; Simonite, T., Matsakis, L.; Martineau, P.; Tiku, N.; Matsakis, L.; Schwartz, O.; Martineau, P. How facial recognition is fighting child sex trafficking. *WIRED*, 2019. Disponível em: https://www.wired.com/story/how-facial-recognition-fighting-child-sex-trafficking/. Acesso em: 25 ago. 2019.

77. Eandt.theiet. *Child abuse targeted with upgraded police tech, limiting officer exposure to images*. Institution of Engineering and Technology, 2019. Disponível em: https://eandt.theiet.org/content/articles/2019/07/child-abuse-targeted-with-upgraded-police-tech-limiting-officer-exposure-to-indecent-images/. Acesso em: 25 ago. 2019.

78. McIntyre, N.; Pegg, D. Councils use 377,000 people's data in efforts to predict child abuse. *The Guardian*, 2019. Disponível em: https://www.theguardian.com/society/2018/sep/16/councils-use-377000-peoples-data-in-efforts-to-predict-child-abuse. Acesso em: 25 ago. 2019.

79. Europol. *Global action tackles distribution of child sexual exploitation images via WhatsApp*: 39 arrested so far. 2019. Disponível em: https://www.europol.europa.eu/newsroom/news/global-action-tackles-distribution-of-child-sexual-exploitation-images-whatsapp-39-arrested-so-far. Acesso em: 25 ago. 2019.

80. DW. *Interpol busts international pedophilia ring*. DW, 23 May 2019. Disponível em: https://www.dw.com/en/interpol-busts-international-pedophilia-ring/a-48841717. Acesso em: 25 ago. 2019.

81. Estatística fornecida pelo INHOPE.

82. Schia, Niels Nagelhus. The cyber frontier and digital pitfalls in the Global South. *Third World Quarterly*, v. 39, n. 5, p. 821-837, 2018. DOI: 10.1080/01436597.2017.1408403}

83. EIU. *Out the shadows: shining light on the response to child sexual abuse and exploitation*. 2019. Disponível em: https://outoftheshadows.eiu.com. Acesso em: 25 ago. 2019.

84. Children and Business. *Children's rights and business principles*. 2019. Disponível em: http://childrenandbusiness.org/. Acesso em: 25 ago. 2019.

85. UNCTAD. *Cybercrime legislation worldwide*. Disponível em: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx. Acesso em: 11 ago. 2019.

86. UNICEF. *COP guidelines for industry*. Disponível em: https://www.unicef.org/csr/COPguidelines.htm Acesso em: 7 set. 2019.

87. EIU. *Out the shadows*: shining light on the response to child sexual abuse and exploitation. 2019. Disponível em: https://outoftheshadows.eiu.com. Acesso em: 25 ago. 2019.

88. Public Safety Canada. *Child pornography offenders*: a review. 2019. Disponível em: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2018-s001/index-en.aspx. Acesso em: 25 ago. 2019.

89. Thorn. *Production and active trading of child sexual exploitation images depicting identified victims*. 2019. Disponível em: https://www.thorn.org/wp-content/uploads/2018/03/Production-and-Active-Trading-of-CSAM_FullReport_FINAL.pdf. Acesso em: 13 ago. 2019.

90. NetClean. *The NetClean report 2017*: there is no such thing as a typical offender. 2018. (The consumer of child sexual abuse material). Disponível em: https://www.netclean.com/netclean-report-2017/insight-3/. Acesso em: 25 ago. 2019.

91. Stop It Now. *Let's talk*: speaking up to prevent child sexual abuse. 2006. Disponível em: https://www.stopitnow.org/sites/default/files/documents/files/lets_talk.pdf.

92. Stone, J.; Stone, J. *The dark web isn't as big as you think*. CyberScoop, 2019. Disponível em: https://www.cyberscoop.com/dark-web-marketplaces-research-recorded-future/. Acesso em: 25 ago. 2019.

93. Ecpat. *Emerging global threats related to the online sexual exploitation of children*. 2019. Disponível em: https://www.ecpat.org/wp-content/uploads/2018/08/Briefing-Paper-Emerging-Issues-and-Global-Threats-Children-online-_06.06.17.pdf. Acesso em: 10 ago. 2019.

94. Stop It Now. *Understanding what makes kids vulnerable to being sexually abused*. 2019. Disponível em: https://www.stopitnow.org/ohc-content/understanding-what-makes-kids-vulnerable-to-being-sexually-abused. Acesso em: 11 ago. 2019.

95. NICE. *NICE guideline NG76*: child abuse and neglect: recognising, assessing and responding to abuse and neglect of children and young people. United Kingdom, 2019. Disponível em: https://www.nice.org.uk/guidance/ng76/evidence/full-guideline-pdf-4607478261. Acesso em: 25 ago. 2019.

96. WHO. *Child abuse and neglect by parents and other caregivers*. Geneva, 2019. Disponível em: https://www.who.int/violence_injury_prevention/violence/global_campaign/en/chap3.pdf. Acesso em: 25 ago. 2019.

97. UNICEF. *'Shame and pain'*: Vietnam starts to grapple with child abuse epidemic. New York, 2019. Disponível em: https://www.unicef.org/vietnam/stories/shame-and-pain-vietnam-starts-grapple-child-abuse-epidemic. Acesso em: 11 ago. 2019.

98. BBC News. *Instagram 'biggest for child grooming online'*. 1 Mar. 2019. Disponível em: https://www.bbc.co.uk/news/uk-47410520. Acesso em: 12 ago. 2019.

99. The Conversation. *YouTube's paedophile problem is only a small part of the internet's issue with child sexual abuse*. 5 Mar. 2019. Disponível em: https://theconversation.com/youtubes-paedophile-problem-is-only-a-small-part-of-the-internets-issue-with-child-sexual-abuse-94126. Acesso em: 12 ago. 2019.

100. Ditch the Label. *Anti-bullying survey 2017*. 2018. Disponível em: https://www. ditchthelabel.org/wp-content/uploads/2017/07/The-Annual-Bullying-Survey-2017-1.pdf. Acesso em: 12 ago. 2019.

101. Linkedin Economic Graph. *LinkedIn workforce report*. United States, Aug. 2018. Disponível em: https://economicgraph.linkedin.com/resources/linkedin-workforce-report-august-2018. Acesso em: 25 ago. 2019.

102. European Union. *Final results of the European Data Market study measuring the size and trends of the EU data economy*. Digital Single Market - European Commission, 2019. Disponível em: https://ec.europa.eu/digital-single-market/en/news/final-results-european-data-market-study-measuring-size-and-trends-eu-data-economy. Acesso em: 25 ago. 2019.

103. Anon. *Data science and analytics skills shortage*: equipping the APEC workforce with the competencies demanded by employers. 2019. Disponível em: https://www.apec.org/Publications/2017/11/Data-Science-and-Analytics-Skills-Shortage. Acesso em: 25 ago. 2019.

104. Thorn. *Sound practices guide to stopping child sexual abuse*. 2019. Disponível em: https://www.thorn.org/sound-practices-guide-stopping-child-abuse/. Acesso em: 7 set. 2019.

105. NetClean. *Benchmarking Index on the response to child sexual abuse and exploitation*. 2019. Disponível em: https://www.netclean.com/2019/01/11/benchmarking-index-response-to-child-sexual-abuse-and-exploitation/. Acesso em: 7 set. 2019.

106. United Kingdom. Legislation. *Data Protection Act 2018*. London, 2018. Disponível em: http://www.legislation. gov.uk/ukpga/2018/12/section/123/enacted. Acesso em: 7 set. 2019.

107. INHOPE. *INHOPE annual report 2017*. Disponível em: http://88.208.218.79/libraries/annual_reports/inhope_annual_ report_2017.sflb.ashx\.

108. ChildSafeNet. *Cyber grooming*. Disponível em: https://www.childsafenet.org/new-page-15.

109. UNESCO. *Violência escolar e bullying*: relatório sobre a situação mundial. Brasília, 2019. p. 8. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000368092?posInSet=1&queryId=d37b8b39-e135-4f7c-9e06-f5a755704f71.

110. Cambridge Dictionary. *By default*. Disponível em: https://dictionary.cambridge.org/us/.

111. Cambridge Dictionary. *By design*. Disponível em: https://dictionary.cambridge.org/us/.

Recursos 15

Recursos

Contigo Conectados Online Safety Resources (ES)
https://contigoconectados.com/resultados/riesgos/

Economist Intelligence Unit: Out of the Shadows
https://outoftheshadows.eiu.com/

End Violence Against Children: Keeping Children Safe Online
https://www.end-violence.org/keeping-children-safe-online

Facebook: Photo Video Matching
https://newsroom.fb.com/news/2019/08/open-source-photo-video-matching/

Facebook: New technology to fight child exploitation
https://newsroom.fb.com/news/2018/10/fighting-child-exploitation/

Griffeye
https://www.griffeye.com/

GSMA European Framework for Safer Mobile Use by Younger Teenagers and Children
https://www.gsma.com/publicpolicy/consumer-affairs/children-mobile-technology/myouth

IMEC Child Sexual Abuse Material: Model Legislation & Global Review
https://www.icmec.org/wp-content/uploads/2018/12/CSAM-Model-Law-9th-Ed-FINAL-12-3-18.pdf

Inhope Global Internet Hotlines
http://www.inhopefoundation.org/

ITU COP Guidelines
https://www.itu.int/en/cop/Pages/guidelines.aspx

ITU Guidelines for Policy Makers on Child Protection
https://www.itu.int/en/cop/Documents/guidelines-policy%20makers-e.pdf

Luxembourg Terminology Guidelines for The Protection of Children from Sexual Exploitation and Sexual Abuse
http://luxembourgguidelines.org/english-version/

Microsoft Digital Skills
https://www.microsoft.com/en-us/digital-skills/online-safety

Microsoft Online Safety Resources
https://www.microsoft.com/en-us/digital-skills/online-safety-resources

Microsoft PhotoDNA
https://www.microsoft.com/en-us/photodna

NetClean
https://www.netclean.com/

OECD: The Future of Education and Skills
https://www.oecd.org/education/2030/E2030%20Position%20Paper%20(05.04.2018).pdf

Online Safety Technical Note
https://www.end-violence.org/online-safety-technical-note

The #ENDviolence Youth Manifesto
https://www.unicef.org/end-violence/youth-manifesto

Thorn
https://www.thorn.org

UK Online Harms White Paper
https://www.gov.uk/government/consultations/online-harms-white-paper

UN Convention on the Rights of the Child
https://www.ohchr.org/en/professionalinterest/pages/crc.aspx

UNICEF & GSMA: NOTICE AND TAKEDOWN — Company policies and practices to remove *online* child sexual abuse material
https://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/notice_and_takedown_gsma_unicef_april_2016.pdf

WeProtect Model National Response Guidance Document
https://www.weprotect.org/the-model-national-response

The ITU Global Cybersecurity Index
https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

NOTAS


BROADBAND COMMISSION
FOR SUSTAINABLE DEVELOPMENT
ITU
UNESCO