

Diretrizes para a Indústria sobre Proteção Infantil Online 2020



Diretrizes para a Indústria sobre Proteção Infantil Online

Agradecimentos

Essas diretrizes foram desenvolvidas pela União Internacional de Telecomunicações (UIT) (*International Telecommunication Union-ITU*) e um grupo de trabalho composto por autores contribuintes de instituições líderes e ativas no setor de tecnologias da informação e comunicação (TIC), assim como em questões de proteção infantil e incluiu a EBU, a Parceria Global pelo Fim da Violência contra Crianças (*Global Partnership to End Violence Against Children*), GSMA, a Aliança Internacional de Pessoas com Deficiência (*International Disability Alliance*), a Internet Watch Foundation (IWF), Privately SA e o UNICEF. O grupo de trabalho foi presidido por Anjan Bose (UNICEF) e coordenado por Fanny Rotino (UIT).

As diretrizes da UIT não seriam possíveis sem a dedicação, o tempo e o entusiasmo dos autores contribuintes. Contribuições inestimáveis também foram recebidas do e-Worldwide Group (e-WWG), Facebook, Tencent Games, Twitter, Walt Disney Company, bem como de outras partes interessadas da indústria, que compartilham o objetivo comum de tornar a Internet um lugar melhor e mais seguro para crianças e jovens. A UIT é grata aos seguintes parceiros, que contribuíram com seu valioso tempo e ideias (listados em ordem alfabética de acordo com os nomes das organizações em inglês):

- Giacomo Mazzone (EBU)
- Salma Abbasi (e-WWG)
- David Miles e Caroline Hurst (Facebook)
- Amy Crocker e Serena Tommasino (Global Partnership to End Violence Against Children)
- Jenny Jones (GSMA)
- Lucy Richardson (International Disability Alliance)
- Fanny Rotino (ITU)
- Tess Leyland (IWF)
- Deepak Tewari (Privately SA)
- Adam Liu (Tencent Games)
- Katy Minshall (Twitter)
- Anjan Bose, Daniel Kardefelt Winther, Emma Day, Josianne Galea Baron, Sarah Jacobstein e Steven Edwin Vosloo (UNICEF)
- Amy E. Cunningham (The Walt Disney Company)

ISBN

978-92-61-30081-4 (Versão em papel)

978-92-61-30411-9 (Versão eletrônica)

978-92-61-30071-5 (Versão EPUB)

978-92-61-30421-8 (Versão Mobi)



Por favor considere o meio ambiente antes de imprimir este documento.

© ITU 2020

Alguns direitos reservados. Este trabalho está licenciado ao público por meio de uma licença Creative Commons Atribuição-Não-Comercial-Compartilhamento pela mesma licença 3.0 IGO (CC BY-NC-SA 3.0 IGO).

De acordo com os termos desta licença, você pode copiar, redistribuir e adaptar o trabalho para fins não comerciais, desde que o trabalho seja adequadamente citado, conforme indicado abaixo. Sempre que este trabalho for utilizado, não deve haver sugestão de que a UIT apoia qualquer organização, produto ou serviço específico. O uso não autorizado de nomes ou logotipos da UIT não é permitido. Caso o trabalho for adaptado, deverá ser licenciado sob a mesma ou equivalente licença Creative Commons.

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

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

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

Porém, o acesso mais amplo e mais fácil a serviços online também apresenta desafios significativos à segurança das crianças - tanto online quanto offline. Desde questões de privacidade, violência entre pares e conteúdo violento e/ou impróprio para a idade, a golpistas na Internet e crimes contra crianças, como aliciamento on-line e abuso e exploração sexual, as crianças de hoje enfrentam muitos graves riscos. As ameaças estão se multiplicando e os perpetradores operam cada vez mais simultaneamente e para além das fronteiras físicas, tornando-os difíceis de rastrear e ainda mais difíceis de responsabilizar.

Além disso, a pandemia global da COVID-19 causou um aumento no número de crianças que ingressam no mundo online pela primeira vez, para continuar seus estudos e manter uma interação social. As restrições impostas pelo vírus não apenas se traduziram em muitas crianças mais novas interagindo online em idades mais tenras do que seus pais planejavam, mas também na necessidade dos pais conciliarem seus compromissos de trabalho e portanto serem incapazes de supervisionar seus filhos, deixando os jovens em risco de acessarem conteúdo inadequado ou serem alvos de criminosos na produção de material pedopornográfico infantil (CSAM- *child sexual abuse material*).

Os criminosos estão lucrando com os avanços tecnológicos, como aplicativos e jogos interconectados, compartilhamento rápido de arquivos, streaming ao vivo, criptomoedas, a Dark Web e software de criptografia robusto. No entanto, eles também lucram com ações muitas vezes descoordenadas e hesitantes por parte do setor de tecnologia no combate eficiente do problema.

As tecnologias emergentes podem fazer parte da solução, por exemplo, o banco de dados de abuso sexual infantil da Interpol, baseado em inteligência artificial, que usa software de comparação de imagens e vídeos para fazer conexões rápidas entre vítimas, abusadores e lugares. Mas a tecnologia sozinha não resolverá o problema.

Para reduzir os riscos da revolução digital e, ao mesmo tempo, permitir que mais e mais jovens colham seus benefícios, uma resposta colaborativa e coordenada de múltiplas partes interessadas nunca foi tão essencial. Governos, sociedade civil, comunidades locais, organizações internacionais e partes interessadas da indústria devem se unir em torno de um propósito comum.

Reconhecendo isso, em 2018, os Estados Membros da UIT solicitaram uma atualização abrangente de nossas diretrizes [sobre proteção infantil online](#). Essas novas diretrizes da UIT foram repensadas, reescritas e redesenhadas para refletir as mudanças muito significativas no cenário digital em que as crianças desta geração se encontram. Além de refletir os novos desenvolvimentos em tecnologias e plataformas digitais, esta nova edição aborda uma lacuna importante: a situação enfrentada pelas crianças com deficiência, para quem o mundo online oferece uma corda de segurança particularmente crucial para assegurar uma plena e gratificante - participação social.

O setor de tecnologia tem um papel crítico e proativo a desempenhar no estabelecimento das bases para um uso mais seguro de serviços da Internet e outras tecnologias, para as crianças de hoje e as gerações futuras.

As empresas devem cada vez mais colocar os interesses das crianças no centro de seu trabalho, prestando especial atenção à proteção da privacidade dos dados pessoais dos jovens usuários, preservando seu direito à liberdade de expressão, combatendo o flagelo crescente de material pedopornográfico infantil (CSAM) e garantindo a existência de sistemas que abordem as violações dos direitos da criança quando ocorrerem.

Em casos em que as leis nacionais ainda não estão alinhadas ao direito internacional, toda empresa tem a oportunidade - e a responsabilidade - de alinhar seus próprios marcos operacionais com os mais altos padrões e as melhores práticas internacionais.

Para a indústria, esperamos que essas diretrizes sirvam como uma base sólida para o desenvolvimento de políticas de negócios e soluções inovadoras. No verdadeiro espírito do papel da UIT como organizadora global, tenho orgulho destas diretrizes serem o produto de um esforço colaborativo global e serem co-escritas por especialistas de uma ampla comunidade internacional.

Também estou muito satisfeito em apresentar nosso novo mascote da **Proteção Infantil Online-PIO** (*PIO-Child Online Protection*), Sango: um personagem amigável, corajoso e destemido projetado inteiramente por um grupo de crianças como parte do novo programa da UIT de extensão internacional para jovens.

Em uma época em que cada vez mais jovens estão online, as diretrizes de proteção infantil da UIT são mais importantes do que nunca. A indústria, os governos, pais e educadores, assim como as próprias crianças, todos têm um papel vital a desempenhar. Estou grato, como sempre, pelo apoio prestado e espero continuar nossa estreita colaboração nesta questão crítica.



Doreen Bogdan-Martin
Diretor
Departamento de Desenvolvimento da Telecomunicação, UIT

Agradecimentos.....	ii
Prefácio	v
1. Visão Geral.....	1
2. O que é proteção infantil online?.....	3
2.1. Informações básicas	6
2.2. Modelos nacionais e transnacionais existentes para Proteção Infantil Online.....	14
3. Principais áreas de proteção e promoção dos direitos da criança.....	17
3.1. Integrar os direitos da criança em todas as políticas corporativas e processos de gestão adequados	17
3.2. Desenvolvimento de processos padronizados para lidar com material de pornografia infantil.....	19
3.3. Criação de um ambiente online mais seguro e adequado à faixa etária	21
3.4. Educar crianças, responsáveis e educadores sobre a segurança das crianças e o uso responsável das TICs.....	24
3.5. Promover a tecnologia digital como um meio para aumentar o engajamento cívico	28
4. Diretrizes gerais para a indústria	30
5. Listas de verificação de recursos específicos	40
5.1. Recurso A: Forneça conectividade, armazenamento de dados e serviços de hospedagem.....	40
5.2. Recurso B: Ofereça conteúdo digital com curadoria	44
5.3. Recurso C: hospedar conteúdo gerado pelo usuário e conectar usuários.....	48
5.4. Recurso D: Sistemas movidos por inteligência artificial.....	54
Referências.....	59
Glossário.....	60

Tabela

Tabela 1: Diretrizes gerais para a indústria	41
Tabela 2: Lista de verificação PIO para o Recurso A: Forneça conectividade, dados e dispositivos de hospedagem	52
Tabela 3: Lista de verificação da PIO para o recurso B: ofereça conteúdo digital com curadoria	55
Tabela 4: Lista de verificação PIO para o recurso C: hospede conteúdo gerado pelo usuário e conecte usuários.....	59
Tabela 5: Lista de verificação PIO para o Recurso D: sistemas acionados por IA.....	67

1 Visão Geral

O objetivo deste documento é fornecer uma orientação para que as partes interessadas da indústria de TIC criem seus próprios recursos para assegurar a proteção infantil online (PIO). O objetivo dessas diretrizes sobre proteção infantil online formatadas para a indústria é fornecer uma estrutura útil, flexível e fácil de usar que inclua tanto as visões empresariais quanto a sua responsabilidade de proteger os usuários. Também visam estabelecer a base para o uso mais seguro dos serviços online e tecnologias associadas para as crianças de hoje e as gerações futuras.

Como uma caixa de ferramentas, essas diretrizes também visam aumentar o sucesso dos negócios, ajudando grandes e pequenas operações e partes interessadas a desenvolver e manter um modelo de negócios atraente e sustentável, que ao mesmo tempo compreenda as responsabilidades legais e morais para com as crianças e a sociedade.

Em resposta aos avanços substanciais em tecnologia e convergência, a UIT, o UNICEF e os parceiros de proteção online infantil desenvolveram e atualizaram as diretrizes para uma ampla gama de empresas que desenvolvem, fornecem ou usam telecomunicações ou atividades relacionadas na entrega de seus produtos e serviços.

As novas diretrizes para a indústria sobre proteção infantil online são o resultado de consultas com membros da Iniciativa da PIO, bem como consultas mais amplas com membros da sociedade civil, empresas, academia, governos, mídia, organizações internacionais e jovens.

O objetivo deste documento é:

- estabelecer um ponto de referência comum e orientação para as indústrias online e de TIC e partes interessadas relevantes;
- fornecer orientação às empresas na identificação, prevenção e mitigação de quaisquer impactos adversos de seus produtos e serviços sobre os direitos das crianças;
- fornecer orientação às empresas sobre como identificar maneiras de promover os direitos da criança e a cidadania digital responsável entre as crianças;
- sugerir princípios comuns para formar a base dos compromissos nacionais ou regionais em todos os setores relacionados, embora reconhecendo que diferentes tipos de negócios usarão diversos modelos de implementação.

Escopo

A proteção infantil online é um desafio complexo que engloba vários aspectos diferentes de governança, política, operacionais, técnicos e jurídicos. Essas diretrizes tentam abordar, organizar e priorizar muitas dessas áreas, com base em modelos, estruturas e outras referências existentes e bem reconhecidas.

As diretrizes enfocam a proteção das crianças em todas as áreas e contra todos os riscos do mundo digital e, como tal, destacam as boas práticas das partes interessadas da indústria que podem ser consideradas no processo de elaboração, desenvolvimento e gestão das políticas de PIO da empresa. Eles fornecem orientação aos atores da indústria não apenas sobre como gerenciar e conter atividades online ilegais contra as quais eles têm o dever de agir (como material pornográfico infantil online) por meio de seus serviços, mas também se concentram em outras questões que podem não ser definidas como crimes em todas as jurisdições. Isso inclui violência entre pares, cyberbullying e assédio online, bem como questões relacionadas

à privacidade ou bem-estar geral, fraude ou outras ameaças, que podem ser prejudiciais às crianças apenas em determinados contextos.

Para tanto, essas diretrizes incluem recomendações sobre boas práticas para enfrentar os riscos que as crianças enfrentam no mundo digital e sobre como agir para estabelecer um ambiente seguro para as crianças online. Estas diretrizes fornecem conselhos sobre como a indústria pode trabalhar para ajudar a garantir a segurança das crianças ao usar TICs, a Internet ou qualquer uma das tecnologias ou dispositivos associados que podem se conectar a ela, incluindo telefones celulares, consoles de jogos, brinquedos conectados, relógios, a Internet das coisas e sistemas acionados por IA. Eles, portanto, fornecem uma visão geral dos principais problemas e desafios relacionados à proteção infantil online e propõem ações para empresas e partes interessadas para o desenvolvimento de políticas locais e internas de PIO. Essas diretrizes não cobrem aspectos como o processo de desenvolvimento real ou a redação que as políticas PIO para a indústria poderiam incluir.

Estrutura

Seção 1 - Visão geral: esta seção destaca a finalidade, o escopo e o público-alvo dessas diretrizes.

Seção 2 - Introdução à proteção infantil online: esta seção apresenta uma visão geral da questão da proteção infantil online, destacando algumas informações básicas, incluindo a situação especial de crianças com deficiência. Além disso, fornece exemplos de modelos internacionais e nacionais existentes para manter as crianças seguras enquanto estão online como possíveis áreas de intervenção para as partes interessadas da indústria.

Seção 3 - Principais áreas de proteção e promoção dos direitos das crianças: Esta seção descreve cinco áreas principais onde as empresas podem tomar medidas para garantir que as crianças façam uso seguro.

Seção 4 - Diretrizes gerais: esta seção fornece recomendações para todas as partes interessadas da indústria sobre a proteção da segurança das crianças ao usar as TICs e a promoção do uso positivo das TICs, incluindo a cidadania digital responsável entre as crianças.

Seção 5 - Listas de verificação relacionadas a recursos específicos: esta seção destaca recomendações específicas para as partes interessadas sobre ações concretas que devem ser tomadas para garantir o respeito e apoiar os direitos da criança, com os seguintes recursos:

- Recurso A: forneça conectividade, armazenamento de dados e serviços de hospedagem
- Recurso B: ofereça conteúdo digital com curadoria
- Recurso C: hospede conteúdo gerado pelo usuário e conecte usuários
- Recurso D: sistemas baseados em IA

Público-alvo

Com base nos Princípios Orientadores das Nações Unidas sobre Negócios e Direitos Humanos¹, os Direitos das Crianças e Princípios Comerciais exigem que as empresas cumpram sua responsabilidade de respeitar os direitos das crianças, evitando quaisquer impactos adversos relacionados às suas operações, produtos ou serviços. Esses Princípios também articulam a diferença entre respeito (o mínimo exigido dos negócios para evitar que as crianças sejam prejudicadas) e apoio (por exemplo, por meio de ações voluntárias que buscam promover

¹ Princípios Orientadores das Nações Unidas sobre Negócios e Direitos Humanos.

a realização dos direitos plenos das crianças). As empresas precisam garantir o direito das crianças à proteção online, bem como ao acesso à informação e à liberdade de expressão, promovendo o uso positivo das TICs pelas crianças.

As distinções tradicionais entre diferentes partes dos setores de telecomunicações e telefonia móvel e entre empresas de Internet e emissoras estão rapidamente se desintegrando e se tornando turvas. A convergência está atraindo esses fluxos digitais antes díspares para uma única corrente que alcança bilhões de pessoas em todas as partes do mundo. Cooperação e parceria são as chaves para estabelecer as bases para um uso mais seguro da Internet e das tecnologias associadas. Governos, setor privado, formuladores de políticas, educadores, sociedade civil, pais e cuidadores, todos têm um papel vital a desempenhar para que o objetivo seja atingido. A indústria pode atuar em cinco áreas principais, conforme descrito na seção 3.

2 O que é proteção infantil online?

Nos últimos 10 anos, o uso e o papel da Internet na vida das pessoas mudaram consideravelmente. Com a prevalência de smartphones e tablets, a acessibilidade da tecnologia Wi-Fi e 4G e o desenvolvimento das plataformas e aplicativos de mídia social, cada vez mais pessoas estão acessando a Internet por motivos cada vez mais variados.

Em 2019, mais da metade da população mundial usava a Internet. A maior proporção de usuários da Internet são pessoas com menos de 44 anos, com um uso igualmente alto entre os de 16 a 24 anos e entre os de 35 a 44 anos. A nível global, um em cada três utilizadores da Internet é uma criança (0-18 anos) e o UNICEF estima que 71 por cento dos jovens já estão online². A proliferação de pontos de acesso à Internet, tecnologia móvel e a crescente variedade de dispositivos habilitados para Internet, combinados com os imensos recursos encontrados no ciberespaço, oferecem oportunidades sem precedentes para aprender, compartilhar e se comunicar.

Os benefícios do uso das TICs incluem um acesso mais amplo a informações sobre serviços sociais, recursos educacionais e conselhos de saúde. À medida que crianças, jovens e famílias usam a Internet e os telefones celulares para buscar informações e assistência, e para relatar incidentes de abuso, essas tecnologias podem ajudar a proteger crianças e jovens da violência e da exploração. Os prestadores de serviços de proteção à criança também usam as TICs para coletar e transmitir dados, facilitando o registro de nascimento, o gerenciamento de casos, o rastreamento de famílias, a coleta de dados e o mapeamento da violência, entre outros.

Além disso, a Internet aumentou o acesso à informação em todos os cantos do globo, permitindo que crianças e jovens pesquisem quase todos os assuntos de interesse, acessem a mídia mundial, persigam suas ambições vocacionais e aproveitem ideias para o futuro. O uso das TICs capacita crianças e jovens a fazerem valer seus direitos e expressar suas opiniões, e também permite que eles se conectem e se comuniquem com suas famílias e amigos. As TICs também servem como um meio fundamental de intercâmbio cultural e uma fonte de entretenimento.

2 OCDE, “[Novas Tecnologias e Crianças do Século 21: Tendências Recentes e Resultados](#)”, Documento de Trabalho sobre Educação No. 179.

Apesar dos profundos benefícios da Internet, as crianças e os jovens também podem entrar em contato com vários riscos ao usar as TICs. Eles podem ser expostos a conteúdo impróprio para a idade ou contato impróprio, incluindo de possíveis perpetradores de abuso sexual. Eles podem sofrer danos à reputação com a publicação de informações pessoais confidenciais on-line ou por meio de "sexting", muitas vezes não conseguindo compreender as implicações de suas ações sobre eles próprios e outros e suas "pegadas digitais" de longo prazo. Eles também enfrentam riscos relacionados à privacidade online decorrentes da coleta de dados e da coleta e uso de informações de localização.

A Convenção sobre os Direitos da Criança, que é o tratado internacional de direitos humanos mais amplamente ratificado³, estabelece os direitos civis, políticos, econômicos, sociais e culturais das crianças. Estabelece que todas as crianças e jovens têm direito à educação; lazer, diversão e cultura; informações apropriadas; liberdade de pensamento e expressão; e privacidade, e para expressar seus pontos de vista sobre questões que os afetam de acordo com suas capacidades em evolução. A Convenção também protege crianças e jovens de todas as formas de violência, exploração, abuso e discriminação de qualquer tipo, e estabelece que o interesse superior da criança deve ser a consideração principal em qualquer assunto que as afete. Pais, responsáveis, educadores e membros da comunidade, incluindo líderes comunitários e atores da sociedade civil, têm a responsabilidade de nutrir e apoiar crianças e jovens em sua passagem para a idade adulta. Os governos têm um papel importante em garantir que todas as partes interessadas cumpram esse papel.

Com relação à proteção dos direitos das crianças online, as indústrias precisam trabalhar juntas para encontrar um equilíbrio cuidadoso entre o direito das crianças à proteção e seu direito de acesso à informação e liberdade de expressão. As empresas devem, portanto, priorizar medidas que protejam crianças e jovens online, que sejam direcionadas e não sejam excessivamente restritivas, seja para a criança ou outros usuários. Além disso, há um consenso crescente de que a promoção da cidadania digital entre crianças e jovens e o desenvolvimento de produtos e plataformas que facilitem o uso positivo das TICs pelas crianças deve ser uma prioridade para o setor privado.

Embora as tecnologias online apresentem muitas oportunidades para crianças e jovens se comunicarem, aprenderem novas habilidades, serem criativas e contribuírem para fazer uma sociedade mais justa para todos, as tecnologias também representam novos riscos para a segurança das crianças e jovens. Podem expor as crianças e jovens a riscos e danos potenciais relacionados a questões de privacidade, conteúdo ilegal, assédio, cyberbullying, uso indevido de dados pessoais ou aliciamento para fins sexuais e até mesmo abuso e exploração sexual infantil. Suas reputações podem ser expostas a danos, incluindo "pornografia de vingança" vinculada à publicação de informações pessoais confidenciais, seja online ou por meio de "sexting", uma forma dos usuários enviarem mensagens, fotografias ou imagens sexualmente explícitas entre telefones celulares. Elas também enfrentam riscos relacionados à sua privacidade quando estão usando a Internet. As crianças, devido à sua idade e ao desenvolvimento da sua maturidade, muitas vezes são incapazes de compreender totalmente os riscos associados ao mundo online e as possíveis repercussões negativas de seu comportamento inadequado para os outros e para si mesmas.

3 Convenção das Nações Unidas sobre os Direitos da Criança. Todos, exceto três países (Somália, Sudão do Sul e os Estados Unidos) ratificaram a Convenção sobre os Direitos da Criança.

Apesar das vantagens, também há desvantagens no uso das tecnologias emergentes mais avançadas. Os desenvolvimentos em IA e machine learning, realidade virtual e aumentada, big data, robótica e a Internet das Coisas devem transformar ainda mais as práticas de uso de mídia de crianças e jovens. Embora essas tecnologias sejam desenvolvidas predominantemente para expandir o escopo da prestação de serviços e aumentar a conveniência (por meio, por exemplo, de assistência por voz, acessibilidade e novas formas de imersão digital), algumas dessas tecnologias podem ter impactos não intencionais e até mesmo ser mal utilizadas por criminosos sexuais infantis para atender às suas necessidades. A criação de um ambiente online seguro para crianças e jovens requer a participação efetiva dos governos, do setor privado e de todas as partes interessadas. Focar nas habilidades digitais e na alfabetização de pais e educadores também deve ser uma das primeiras metas, em prol da qual a indústria pode desempenhar um papel vital e sustentável.

Algumas crianças podem ter uma boa compreensão dos riscos do ambiente online e como reagir a eles. No entanto, isso não pode ser dito de todas as crianças em todos os lugares, especialmente entre os grupos vulneráveis. De acordo com a meta 16.2 dos Objetivos de Desenvolvimento Sustentável das Nações Unidas, que visa acabar com o abuso, exploração, tráfico e todas as formas de violência e tortura contra crianças, a proteção de crianças online é vital.

Desde 2009, a Iniciativa PIO, um esforço internacional com várias partes interessadas estabelecido pela UIT, tem como objetivo aumentar a conscientização sobre os riscos da internet para as crianças e as possíveis respostas a esses riscos. A iniciativa reúne parceiros de todos os setores da comunidade global para garantir uma experiência online segura para crianças em todos os lugares. Como parte da Iniciativa, em 2009 a UIT publicou um conjunto de diretrizes da PIO para quatro grupos: crianças; pais, responsáveis e educadores; indústria; e formuladores de políticas. A proteção infantil online é entendida nestas diretrizes como uma abordagem abrangente para responder a todas as ameaças e danos potenciais que crianças e jovens podem encontrar online ou que sejam facilitados por tecnologias online. Neste documento, a proteção infantil online também abrange danos a crianças que ocorrem offline, mas estão vinculados a evidências de violência e abuso online. Além de levar em consideração o comportamento e as atividades on-line das crianças, a proteção infantil on-line também se refere ao uso indevido de tecnologia por pessoas que não sejam as próprias crianças para explorar as crianças.

Todas as partes interessadas relevantes têm o papel de ajudar crianças e jovens a se beneficiarem das oportunidades que a Internet pode oferecer, ao mesmo tempo em que adquirem conhecimento digital e resiliência em relação ao seu bem-estar e proteção online.

Proteger as crianças e jovens é a responsabilidade de todas as partes interessadas. Para que isso aconteça, os formuladores de políticas, a indústria, os pais, responsáveis, educadores e outras partes interessadas devem garantir que as crianças e os jovens possam realizar o seu potencial tanto online como offline.

Embora não haja uma definição universal, a proteção on-line de crianças representa uma abordagem holística para construir espaços digitais seguros, adequados à idade, inclusivos e participativos para crianças e jovens, caracterizados por:

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

Além disso, devido aos rápidos avanços na tecnologia e na sociedade e à natureza sem fronteiras da Internet, a proteção on-line infantil precisa ser ágil e adaptável para que seja eficaz. Novos desafios surgirão com o desenvolvimento de inovações tecnológicas e estes desafios variam de região para região. A melhor maneira de lidar com isso será trabalhando em conjunto como uma comunidade global, à medida que novas soluções para esses desafios precisam ser encontradas.

2.1 Informações básicas

Como a Internet está totalmente integrada na vida de crianças e jovens, é impossível considerar o mundo digital e físico separadamente.

Essa conectividade tem sido extremamente fortalecedora. O mundo online permite que crianças e jovens superem desvantagens e deficiências, e oferece novas arenas de entretenimento, educação, participação e construção de relacionamentos. As plataformas digitais atuais são usadas para uma variedade de atividades e muitas vezes também são experiências multimídia.

⁴Ter acesso e aprender a usar e navegar por essas tecnologias é considerado fundamental para o desenvolvimento dos jovens e as TICs são usadas pela primeira vez em uma idade precoce. Portanto, é crucial que todos os atores estejam cientes de que crianças e jovens muitas vezes começam a usar plataformas e serviços antes de atingirem a idade mínima definida a qual a indústria de tecnologia é obrigada a cumprir e, portanto, a educação deve ser integrada em todos os serviços online usados por crianças ao lado de medidas de proteção.

2.1.1 Crianças no mundo digital

O acesso à Internet

Em 2019, mais da metade da população mundial usava a Internet (53,6 por cento), com uma estimativa de 4,1 bilhões de usuários. Em nível global, um em cada três usuários da Internet é uma criança menor de 18 anos¹. De acordo com o UNICEF, em todo o mundo, 71 por cento dos jovens já estão online². Apesar dos requisitos de idade mínima, o Ofcom (regulador de comunicações do Reino Unido) estima que quase 50 por cento das crianças entre 10 e 12 anos já possuem uma conta nas redes sociais³. As crianças e os jovens são agora uma presença significativa, permanente e persistente na Internet. A Internet serve a outros fins sociais, econômicos e políticos e tornou-se um produto ou serviço familiar ou de consumo, parte integrante da maneira como as famílias, crianças e jovens vivem suas vidas.

Em 2017, a nível regional, o acesso de crianças e jovens à Internet esteve fortemente associado à taxa de rendimento nacional. Os países de baixa renda tendem a ter níveis mais baixos de usuários infantis da Internet do que os países de alta renda. Crianças e jovens na maioria dos países passam mais tempo online nos finais de semana do que durante dias de semana, com adolescentes de 15 a 17 anos passando os períodos mais longos online, entre 2,5 e 5,3 horas, dependendo do país.

- 1 Livingstone, S., Carr, J., and Byrne, J. (2015) One in three: The task for global internet governance in addressing children's rights. Global Commission on Internet Governance: Paper Series, Londres: CIGI e Chatham House, <https://www.cigionline.org/publications/one-three-internet-governance-and-childrens-rights>.
- 2 Broadband Commission, "Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online (2019)," *Broadband Commission for Sustainable Development*, outubro de 2019, 84, https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf.
- 3 BBC, "Under-age social media use on the rise, says Ofcom".

Uso da Internet

Entre crianças e jovens, o dispositivo de acesso à Internet mais popular é o celular, seguido por desktops e laptops. Crianças e jovens passam em média duas horas por dia online durante a semana e quatro horas todos os dias do fim de semana. Embora alguns se sintam permanentemente conectados, muitos outros ainda não têm acesso à Internet em casa. Na prática, a maioria das crianças e jovens que usam a Internet têm acesso por meio de mais de um dispositivo, sendo que aqueles que se conectam pelo menos semanalmente às vezes usam até três dispositivos diferentes. Crianças mais velhas e de países ricos geralmente usam mais dispositivos, e meninos usam um pouco mais dispositivos do que as meninas em todos os países pesquisados.

A atividade mais popular entre meninas e meninos é assistir a vídeos online. Mais de três quartos das crianças e jovens que usam a Internet relatam assistir a vídeos online pelo menos uma vez por semana, sozinhos ou com outros membros de suas famílias. Muitas crianças e jovens podem ser considerados “socializadores ativos”, utilizando várias plataformas de mídia social como Facebook, Twitter, TikTok ou Instagram. Crianças e jovens também se envolvem na política online e fazem sua voz ser ouvida por meio de blogs.

O nível geral de participação em jogos online varia de país para país, de acordo com a facilidade de acesso à Internet para crianças e jovens. No entanto, a disponibilidade e acessibilidade dos jogos online está mudando rapidamente e a idade das crianças e jovens que acessam os jogos online pela primeira vez está diminuindo.

Semanalmente, 10-30 por cento das crianças e jovens usuários da Internet - consultados em um conjunto selecionado de países - participam de atividades online criativas.¹ Para fins educativos, muitas crianças e jovens de todas as idades usam a Internet para fazer o dever de casa, ou mesmo para se atualizar depois de faltar às aulas ou buscar informações sobre saúde online, semanalmente. As crianças mais velhas parecem ter mais apetite por informações do que as mais novas.

¹ Livingstone, S., Kardefelt Winther, D. e Hussein, M. (2019). Global Kids Online Comparative Report Escritório de Pesquisa do UNICEF - Innocenti, Florença, <https://www.unicef-irc.org/publicações/1059-global-kids-online-comparative-report.html>.

Exploração e abuso sexual infantil online

A exploração e o abuso sexual infantil online (CSEA- *Child sexual exploitation and abuse*) estão aumentando a uma taxa surpreendente. Uma década atrás, havia menos de um milhão de arquivos de material de abuso infantil denunciados. Em 2019, esse número subiu para 70 milhões, um aumento de quase 50% em relação aos números de 2018. Além disso, pela primeira vez, os vídeos de abuso superaram o número de fotos nos relatórios às autoridades, mostrando a necessidade de novas ferramentas para lidar com essa tendência. As vítimas de abuso sexual infantil online se enquadram em todas as faixas etárias, mas são cada vez mais jovens. Em 2018, a rede de linhas diretas do INHOPE observou uma mudança no perfil das vítimas de púberes para pré-púberes. Além disso, uma pesquisa da ECPAT International e da INTERPOL em 2018 revelou que as crianças mais novas tinham maior probabilidade de sofrer abusos graves, incluindo tortura, estupro violento ou sadismo. Isso inclui bebês com apenas alguns dias, semanas ou meses de idade. Embora as meninas sejam mais afetadas, o abuso de meninos pode ser mais grave. O mesmo relatório mostra que 80 por cento das vítimas mencionadas nos relatórios eram meninas e 17 por cento eram meninos. Crianças de ambos os sexos foram mencionadas em 3 por cento dos relatórios avaliados.¹

Recorte de Dados²

- Um em cada três usuários da Internet em todo o mundo é criança.
- A cada meio segundo, uma criança se conecta à Internet pela primeira vez.
- 800 milhões de crianças usam as redes sociais.
- A qualquer momento, estima-se que 750.000 pessoas online procuram se conectar com crianças para fins sexuais.
- Existem mais de 46 milhões de imagens ou vídeos únicos de material de pornografia infantil no repositório EUROPOL.
- Mais de 89 por cento das vítimas têm entre 3 e 13 anos.

Para obter mais informações sobre a escala e a resposta ao abuso e exploração infantil online, consulte [a WePROTECT Global Alliance](#). ECPAT e Interpol, "Towards a Global Indicator on Unidentified Victims in Child Sexual

1 Exploitation Material: summary report", 2018.

2 End Violence Against Children, "Safe Online".

2.1.2 O impacto de diferentes plataformas nas experiências digitais das crianças

A Internet e a tecnologia digital apresentam oportunidades e riscos para crianças e jovens. Alguns deles são descritos abaixo.

Quando as crianças usam as mídias sociais, elas se beneficiam de muitas oportunidades para explorar, aprender, comunicar e desenvolver habilidades essenciais. As redes sociais são vistas pelas crianças como plataformas que lhes permitem explorar sua identidade pessoal em um ambiente seguro. Ter as competências relevantes e saber como lidar com questões relacionadas com privacidade e reputação é importante para os jovens.

"Eu sei que tudo que você posta na Internet fica para sempre e pode afetar sua vida no futuro", menino de 14 anos, Chile.

No entanto, com pesquisas mostrando que a maioria das crianças usa a mídia social antes dos 13 anos de idade mínima e os serviços de verificação de idade são geralmente fracos ou inexistentes, os riscos que as crianças enfrentam podem ser sérios. Além disso, embora as crianças queiram aprender habilidades digitais, se tornarem cidadãos digitais e controlar as configurações de privacidade, elas tendem a considerar a privacidade em relação a seus amigos e conhecidos - "O que meus amigos podem ver?" - e menos em relação a estranhos e terceiros. Isso, combinado com a curiosidade natural das crianças e geralmente mais baixo limiar de risco, pode torná-las vulneráveis a aliciamento, exploração, bullying ou outros tipos de conteúdo ou contato prejudicial.

A ampla popularidade do compartilhamento de imagens e vídeos por meio de aplicativos móveis e, particularmente, o uso de plataformas de transmissão ao vivo por crianças, apresenta outras preocupações e riscos à privacidade. Algumas crianças estão produzindo imagens sexuais de si mesmas, de amigos e irmãos e então compartilham online. Em 2019, quase um terço (29 por cento) de todas as páginas da web legendadas pela Internet Watch Foundation-IWF continham imagens autogeradas. Destes, 76 por cento mostraram meninas com idades entre 11-13, a maioria em seus quartos ou outro cômodo da casa. Para alguns, principalmente crianças mais velhas, isso pode ser visto como a exploração natural da sexualidade e da identidade sexual, enquanto para outros, especialmente as crianças mais novas, muitas vezes há coerção por um adulto ou outra criança. Seja qual for o caso, o conteúdo resultante é ilegal em muitos países e pode expor as crianças ao risco de um processo judicial ou ser usado para explorar, preparar ou extorquir a criança.

Da mesma forma, **os jogos online** permitem que as crianças cumpram seu direito fundamental de jogar, bem como construir redes, passar tempo com amigos antigos e conhecer novos, assim como desenvolver habilidades importantes. Embora isso possa ser extremamente positivo, em alguns casos, quando deixadas sem monitoramento e sem o suporte de um adulto responsável, as plataformas de jogos também podem representar riscos para as crianças. Isso inclui jogar excessivamente, riscos financeiros associados a compras excessivas no jogo, coleta e monetização de dados pessoais de crianças por atores da indústria, cyberbullying, discurso de ódio, violência e exposição a conduta ou conteúdo impróprio, aliciamento, uso de imagens reais, geradas no computador ou até imagens de realidade virtual e vídeos que retratam e normalizam o CSEA. Esses riscos não se restringem exclusivamente ao ambiente do jogo, se aplicam também a outros ambientes digitais onde as crianças passam o tempo.

Além disso, os desenvolvimentos na tecnologia levaram ao surgimento da **"Internet das Coisas"**, onde um número e variedade cada vez maior de dispositivos conectados à Internet são capazes de se comunicar e se conectar através da internet. Isso inclui brinquedos, monitores para bebês e dispositivos alimentados por IA que podem apresentar riscos em termos de privacidade e contato indesejado.

Boa prática: Pesquisa

No contexto do cyberbullying, a Microsoft conduziu pesquisas sobre segurança digital e cyberbullying. Em 2012, entrevistou crianças de 8 a 17 anos em 25 países sobre comportamento negativo online. Os resultados mostraram que, em média, 54 por cento dos participantes indicaram que se preocupavam com intimidação online; 37 por cento indicaram que foram vítimas de cyberbullying; e 24 por cento revelaram ter intimidado alguém. A mesma pesquisa demonstrou que menos de três em cada 10 pais haviam discutido o bullying online com seus filhos. Desde 2016, a Microsoft tem conduzido **pesquisas regulares** sobre riscos online, [fornecendo relatórios anuais do Índice de Cívica Digital \(Digital Civility Index Reports\)](#).

[FACES](#) é um programa de multimídia produzido pela NHK Japan e por um consórcio de várias emissoras de serviço público que contém histórias de vítimas de bullying online e offline em todo o mundo. Uma série de retratos de adolescentes em que os protagonistas explicam perante a câmera como reagiram a ataques pela Internet. A série, produzida também em clipes de dois minutos, foi adotada pelo Facebook, UNESCO e o [Conselho da Europa](#) e está disponível em vários idiomas.

Em 2019, o UNICEF publicou um documento de discussão sobre [Direitos da Criança e Jogos Online: Oportunidades e Desafios para Crianças e a Indústria \(Child Rights and Online Gaming: Opportunities and Challenges for Children and the Industry\)](#) para abordar as oportunidades e desafios para crianças em uma das indústrias de entretenimento que cresce mais rapidamente. O artigo explora os seguintes tópicos:

- Direito das crianças à brincar e ter liberdade de expressão (tempo de jogo e resultados de saúde);
- Não discriminação, participação e proteção contra abusos (interação social e inclusão, ambientes tóxicos, limites e verificação de idade, proteção contra aliciamento e abuso sexual);
- O direito à privacidade e à ser livre de exploração econômica (modelos de negócios que demandam dados para acesso, jogos gratuitos e monetização, falta de transparência no conteúdo comercial).

Boa prática: Tecnologia

O Laboratório de ação de realidade virtual do Google (Google Virtual Reality Action Lab) examina como a realidade virtual pode ajudar a incentivar os jovens a se tornarem defensores contra o bullying tanto online como offline.¹

Em setembro de 2019, a BBC lançou um aplicativo móvel chamado [Own IT](#), um aplicativo de bem-estar voltado para crianças de 8 a 13 anos que recebem seu primeiro smartphone. O aplicativo faz parte do compromisso da BBC em apoiar os jovens no ambiente de mídia em constante mudança e segue o lançamento bem-sucedido do site Own IT em 2018. O aplicativo combina tecnologia de machine learning de última geração para monitorar as atividades das crianças em seus smartphones com a opção das crianças relatarem seu estado emocional. Ele usa essas informações para fornecer conteúdo personalizado e intervenções que ajudem as crianças a se manterem felizes e saudáveis enquanto estão online, oferecendo estímulos amigáveis e de apoio quando seu comportamento foge do normal. Os usuários podem acessar o aplicativo para procurar ajuda, mas também está disponível para dar conselhos e suporte instantâneos na tela quando precisarem, por meio de um teclado especialmente desenvolvido. Os recursos incluem:

- Um lembrete aos usuários para que pensem duas vezes antes de compartilhar detalhes pessoais, como números de celular nas redes sociais.
- Auxílio para que usuários entendam como as mensagens podem ser percebidas por outras pessoas, antes de clicarem em enviar.
- Um recurso que rastreia seu humor ao longo do tempo e oferece orientação sobre como melhorar a situação, se necessário.
- Fornece informações sobre tópicos como o uso de telefones à noite e o impacto no bem-estar dos usuários.

O aplicativo apresenta conteúdo especialmente encomendado por toda a BBC. Fornece materiais e recursos úteis para ajudar os jovens a obter o máximo de proveito do seu tempo online e a desenvolver comportamentos e hábitos online saudáveis. Ajuda jovens e pais a ter conversas mais construtivas sobre suas experiências online, mas não fornece relatórios ou feedback aos pais e nenhum dado sai dos dispositivos dos usuários. O aplicativo não coleta nenhum dado pessoal ou conteúdo gerado pelo usuário, pois todo o machine learning é executado no aplicativo e no dispositivo do usuário. [As máquinas são treinadas](#) separadamente sobre os dados de treinamento para garantir que não haja violações de privacidade.

1 Para obter mais informações, consulte Alexa Hasse et al., "[Youth and Cyberbullying: Another Look](#)";, Berkman Klein Center for Internet & Society, 2019.

2.1.3 A situação especial das crianças com deficiência⁵

Crianças e jovens com deficiência enfrentam riscos online da mesma forma que aqueles sem deficiência, mas, além disso, podem enfrentar riscos específicos relacionados às suas deficiências. Crianças e jovens com deficiência frequentemente enfrentam exclusão, estigmatização e barreiras (físicas, econômicas, sociais e de atitude) no acesso às suas comunidades. Essas experiências podem impactar negativamente a criança com deficiência e levá-la a buscar contatos sociais, interações e amizades em espaços online. Embora essas interações possam ser positivas, ajudando a construir auto-estima e criando redes de apoio, elas também podem colocar essas crianças em maior risco de incidentes de aliciamento, solicitação online e/ou assédio sexual. A pesquisa mostra que crianças e jovens com dificuldades offline e aqueles afetados por dificuldades psicossociais correm maior risco de enfrentar tais incidentes⁶.

No geral, as crianças que são vítimas offline provavelmente serão vítimas online. Isso coloca as crianças com deficiência em maior risco online, mas elas têm uma necessidade maior de estar no espaço online. Pesquisas mostram que crianças com deficiência têm maior probabilidade de sofrer abusos de qualquer tipo⁶, especificamente vitimização sexual⁷. A vitimização pode incluir intimidação, assédio, exclusão e discriminação com base na deficiência real ou percebida de uma criança ou em aspectos relacionados à sua deficiência, como a maneira como se comporta ou fala, ou os equipamentos ou serviços que usa.

Os perpetradores de aliciamento, solicitação online e/ou assédio sexual contra crianças e jovens com deficiência podem incluir não apenas criminosos preferenciais que visam crianças e jovens, mas também aqueles que visam crianças e jovens com deficiência. Esses criminosos podem incluir "devotos" - pessoas sem deficiência que são sexualmente atraídas por pessoas com deficiência (mais comumente amputados e pessoas que usam auxílios de locomoção), alguns dos quais até fingem ser deficientes⁸. As ações dessas pessoas podem incluir o download de fotos e vídeos de crianças e jovens com deficiência (que são inócuos por natureza) e/ou seu compartilhamento por meio de fóruns específicos ou contas de mídia social. As ferramentas de denúncia em fóruns e mídias sociais muitas vezes não têm um caminho apropriado para lidar com tais ações.

Há preocupações de que o "compartilhamento" (pais compartilhando informações e fotos de seus filhos e jovens online) pode violar a privacidade de uma criança, causar bullying e constrangimento, ou ter consequências negativas no futuro.⁹ Alguns pais de crianças com deficiência podem compartilhar informações ou mídia de seus filhos em busca de apoio ou conselho e, como resultado, colocam seus filhos em risco de violações de privacidade agora

5 Consulte o Conselho da Europa, "Two clicks forward and one click back: report on children with disabilities in the digital environment", 2019

6 Andrew Schrock et al., "Solicitation, Harassment and Problematic Content", Berkman Center for Internet & Society, 2008.

7 Katrin Mueller-Johnson et al., "Sexual Victimization of Youth with a Physical Disability: An Examination of Prevalence Rates, and Risk and Protective Factors", Journal of Interpersonal Violence, 2014.

8 Richard L Bruno, "Devotees, Pretenders and Wannabes: Two Cases of Factitious Disability Disorder", Sexuality and Disability, 1997.

9 UNICEF, "Child Privacy in the Age of Web 2.0: challenges and opportunities for Policy", Innocenti Discussion Paper 2017-03.

e no futuro. Esses pais também correm o risco de serem alvos de pessoas desinformadas ou sem escrúpulos que oferecem tratamentos, terapias ou “curas” para a deficiência de uma criança. Da mesma forma, alguns pais de crianças e jovens com deficiência podem ser superprotetores devido à falta de conhecimento sobre a melhor forma de orientar o uso que seus filhos fazem da internet ou protegê-los de intimidação ou assédio¹⁰.

Algumas crianças e jovens com deficiência podem enfrentar dificuldades no uso, ou mesmo exclusão de, ambientes online devido a designs inacessíveis (por exemplo, aplicativos que não permitem que o tamanho do texto seja aumentado), negação de acomodações solicitadas (por exemplo, software de leitura de tela ou controles de computador adaptados), ou a necessidade de suporte apropriado (por exemplo, treinamento sobre como usar o equipamento, suporte individual para navegar as interações sociais)¹¹.

2.2 Modelos nacionais e transnacionais existentes para Proteção Infantil Online

A nível global, vários modelos estão sendo adotados para proteger crianças e jovens enquanto estão online. As partes interessadas da indústria devem considerá-los como orientações para iniciativas internacionais e como uma estrutura para garantir que eles não poupem esforços para proteger crianças e jovens online. A indústria da Internet é uma arena diversificada e complexa, composta por empresas de diferentes tamanhos e funções. É essencial que a proteção da criança seja abordada não apenas por plataformas e serviços baseados em conteúdo, mas também por aqueles que são responsáveis pela infraestrutura da Internet.

Deve-se notar que a capacidade de uma indústria introduzir uma política abrangente de proteção à criança é limitada aos recursos disponíveis. Essas diretrizes, portanto, recomendam que as indústrias trabalhem juntas para implantar serviços para proteger os usuários. Ao compartilhar recursos e experiência em engenharia, as indústrias seriam capazes de criar “espaços seguros” de maneira mais eficaz para evitar abusos.

Cooperação da indústria

A [Coalizão de Tecnologia](#) (Technology Coalition) é um exemplo de uma cooperação bem-sucedida entre as partes interessadas da indústria para combater o abuso sexual infantil online.

Modelos transnacionais

As indústrias devem incluir diretrizes internacionais relevantes em seus programas estruturais, bem como cumprir qualquer legislação nacional ou transnacional relevante que se aplique nos países em que operam. As indústrias devem considerar não apenas as ações que devem tomar a nível legal, mas também as atividades que podem realizar e, quando possível, buscar implementar iniciativas globalmente. Alguns dos modelos que fornecem princípios para tais iniciativas incluem:

- [Princípios voluntários ministeriais de cinco países para combater a CSEA online](#) (Ministerial Voluntary principles to counter online CSEA 2020);

10 UNICEF, “[Is there a ladder of children’s online participation?](#)”, Innocenti Research Brief, 2019.

11 Para obter orientações sobre esses direitos, consulte a [Convenção das Nações Unidas sobre os Direitos das Pessoas com Deficiência e o Protocolo Opcional](#), especialmente o Artigo 9 sobre acessibilidade e o Artigo 21 sobre liberdade de expressão e opinião e acesso à informação.

- Broadband Commission for Sustainable Development, Segurança Infantil Online: Minimizando o Risco da Violência, Abuso de Exploração Online ([Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online 2019](#));
- WePROTECT Global Alliance, Uma Resposta Estratégica Global à Exploração Sexual Infantil Online e Abuso (*A Global Strategic Response to Online Child Sexual Exploitation and Abuse*, 2019);
- Parceria Global para Acabar com a Violência contra Crianças, Aprendizado Seguro: Chamada a Ação ([Safe to Learn: Call to Action](#));
- Child Dignity in the Digital World, Aliança de Dignidade Infantil: Relatório do Grupo de Trabalho de Tecnologia (*Child Dignity Alliance: Technology Working Group Report 2018*);
- Diretiva (UE) 2018/1808 do Parlamento Europeu e do Conselho: Diretiva de serviços de mídia audiovisual;
- Regulamento Geral de Proteção de Dados da Comissão Europeia (2018);
- Recomendação da OCDE sobre Proteção de Crianças Online (2012).

Modelos nacionais

Existem vários modelos nacionais e internacionais que definem de forma clara as funções e responsabilidades da indústria de tecnologia na abordagem da proteção infantil online. Alguns deles não são especificamente personalizadas para crianças, mas podem se aplicar a elas como usuárias da Internet. Eles fornecem diretrizes abrangentes para a indústria em relação às políticas regulatórias, padrões e colaboração com outros setores. Para os fins deste documento, são destacados os princípios-chave de tais modelos, conforme se aplicam à indústria de TIC.

O Código de Design Adequado à Faixa Etária, Reino Unido

No início de 2019, o Escritório do Comissário da Informação publicou propostas para seu código de design adequado à faixa etária sobre a proteção dos dados de crianças. O código proposto é baseado no maior interesse da criança, conforme estabelecido na Convenção das Nações Unidas sobre os Direitos da Criança, e estabelece várias expectativas para a indústria. O código consiste em quinze padrões, incluindo serviços de localização desativados de forma predefinida para crianças, de forma que a indústria colete e retenha apenas a quantidade mínima de dados pessoais de crianças, para que o design dos produtos garanta privacidade e para que as explicações sejam adequadas à idade e acessíveis.

O Decreto de Comunicações Digitais Prejudiciais, Nova Zelândia

A Lei de 2015 tornou o abuso cibernético um crime específico e se concentra em uma ampla gama de danos, desde o cyberbullying até a pornografia de vingança. Visa dissuadir, prevenir e diminuir a comunicação digital prejudicial, tornando ilegal a publicação de uma comunicação digital com a intenção de causar sofrimento emocional grave a outra pessoa, e estabelece uma série de 10 princípios de comunicação. Ele capacita os usuários a reclamar para uma organização independente se esses princípios forem violados ou solicitar ordens judiciais contra o autor ou o host da comunicação se o problema não for resolvido.

O Comissário de eSegurança, Austrália

Estabelecido em 2015, o Comissário de eSegurança da Austrália (eSafety Commissioner) é a primeira agência governamental do mundo dedicada a combater o abuso e manter seus cidadãos mais seguros online. Como regulador nacional independente de segurança online,

o eSafety possui uma poderosa combinação de funções. Que vão desde a prevenção até a conscientização, educação, pesquisa e orientação de melhores práticas, até a intervenção precoce e remediação de danos por meio de vários esquemas regulamentares legais que dão ao eSafety o poder de remover rapidamente comunicações de cyberbullying, abuso baseado em imagens e conteúdo ilegal online. Essa ampla área de atuação permite que o eSafety trate da segurança on-line de maneira multifacetada, holística e proativa.

Em 2018, a eSafety desenvolveu o Safety by Design - SbD (Design de Segurança), uma iniciativa que coloca a segurança e os direitos dos usuários no centro da concepção, desenvolvimento e implantação de produtos e serviços online. Um conjunto de princípios de design de segurança está no cerne da iniciativa, estabelecendo medidas realistas e viáveis para garantir que a indústria se comprometa a melhor proteger e salvaguardar os cidadãos online. Os três princípios gerais são:

- 1) Responsabilidades do provedor de serviço:** o ônus da segurança nunca deve recair exclusivamente sobre o usuário final. Medidas preventivas podem ser tomadas para garantir que danos conhecidos e previstos tenham sido avaliados durante o desenvolvimento e fornecimento de um serviço online, junto com medidas para tornar os serviços menos propensos a facilitar, inflamar ou encorajar comportamentos ilegais e inadequados.
- 2) Empoderamento e autonomia do usuário:** a dignidade dos usuários e seus melhores interesses são de importância central. A agência humana e a autonomia devem ser apoiadas, ampliadas e fortalecidas pelo design do serviço, permitindo aos usuários maior controle, governança e regulamentação de suas próprias experiências.
- 3) Transparência e responsabilidade:** essas são as marcas de uma abordagem robusta de segurança, que fornece garantias de que os serviços estão operando de acordo com seus objetivos de segurança publicados, bem como educa e capacita o público sobre as medidas que podem ser tomadas para lidar com questões de segurança.

WePROTECT Global Alliance

No cerne da estratégia da Aliança Global WePROTECT ([WePROTECT Global Alliance](#)) está o apoio aos países no desenvolvimento de respostas coordenadas de múltiplas partes interessadas para combater a exploração sexual infantil online, guiadas por seu Modelo de Resposta Nacional, que atua como um modelo de ação nacional. O modelo fornece uma estrutura a qual os países podem recorrer para combater a exploração sexual infantil online. Dentro do Modelo de Resposta Nacional WePROTECT, há um conjunto claro de compromissos de empresas de TIC relacionados a:

- procedimentos de notificação e remoção;
- relatar exploração e abuso sexual infantil online;
- desenvolver soluções de tecnologia; e
- investir em programas preventivos de PIO eficazes e serviços de resposta.

A Parceria Global para Acabar com a Violência contra as Crianças

A [Parceria Global e o Fundo para Acabar com a Violência contra Crianças](#) (*Global Partnership and Fund to End Violence against Children*) foram lançados pelo Secretário-Geral das Nações Unidas em 2016 com um objetivo: catalisar e apoiar ações para acabar com todas as formas de violência contra crianças até 2030 por meio de uma colaboração única de mais de 400 parceiros de todos setores.

O foco do trabalho está no resgate e apoio às vítimas, soluções de tecnologia para detectar e prevenir as ofensas e crimes, apoio à aplicação da lei, reformas legislativas e políticas e geração de dados e evidências sobre a escala e natureza da CSEA online, bem como compreender as perspectivas das crianças.¹²

3 Principais áreas de proteção e promoção dos direitos da criança

Esta seção descreve cinco áreas principais onde as empresas podem tomar medidas para proteger a segurança de crianças e jovens ao usarem as TICs assim como promover o uso positivo das TICs.

3.1 Integrar os direitos da criança em todas as políticas corporativas e processos de gestão adequados

A integração das considerações sobre os direitos da criança requer que as empresas tomem medidas adequadas para identificar, prevenir, mitigar e, quando apropriado, remediar potenciais e reais impactos adversos sobre os direitos das crianças. Os Princípios Orientadores das Nações Unidas sobre Negócios e Direitos Humanos conclamam todas as empresas e indústrias a estabelecer políticas e processos apropriados para cumprir sua responsabilidade de respeitar os direitos humanos.

As indústrias devem prestar especial atenção às crianças e jovens como um grupo vulnerável no que diz respeito à proteção de dados e à liberdade de expressão. A Resolução 68/167 da Assembleia Geral das Nações Unidas sobre o direito à privacidade na era digital reafirma o direito à privacidade e à liberdade de expressão e a garantia de não ser sujeito a interferências ilegais. Além disso, a Resolução 32/13 do Conselho de Direitos Humanos das Nações Unidas sobre a promoção, proteção e gozo dos direitos humanos na Internet, reconhece a natureza global e aberta da Internet como uma força motriz que acelera o progresso em direção ao desenvolvimento e afirma que os mesmos direitos das pessoas que estão offline também devem ser protegidas online. Em Estados onde há falta de estruturas jurídicas adequadas para a proteção dos direitos de crianças e jovens à privacidade e à liberdade de expressão, as empresas devem seguir a devida diligência para garantir que as políticas e práticas estejam em conformidade com o direito internacional. À medida que o engajamento cívico dos jovens continua a aumentar por meio das comunicações online, as empresas têm uma responsabilidade maior de respeitar os direitos das crianças e dos jovens, mesmo quando as leis nacionais ainda não estão a par dos padrões internacionais.

12 Para obter mais informações, consulte End Violence Against Children, "Grantees of the End Violence Fund".

As empresas devem ter implementado um mecanismo de ouvidoria operacional para fornecer um canal para que os indivíduos afetados levantem questões sobre possíveis violações. Os mecanismos operacionais devem ser acessíveis às crianças, suas famílias e aqueles que representam seus interesses. O Princípio 31 dos Princípios Orientadores sobre Empresas e Direitos Humanos esclarece que tais mecanismos devem ser legítimos, acessíveis, previsíveis, equitativos, transparentes, compatíveis com os direitos, uma fonte de aprendizagem contínua e baseados no engajamento e no diálogo. Juntamente com os processos internos para lidar com os impactos negativos, os mecanismos de ouvidoria devem garantir que as empresas tenham estruturas em vigor para garantir que crianças e jovens tenham recursos adequados quando seus direitos estiverem sob ameaça.

Quando as empresas adotam uma abordagem de segurança para TICs baseada em conformidade, que se concentra no cumprimento da legislação nacional, seguindo a orientação internacional em casos aonde a legislação nacional não existe, evitando impactos adversos sobre os direitos das crianças e jovens, as empresas promovem proativamente o desenvolvimento e o bem-estar das crianças e jovens, sendo por meio de ações voluntárias que promovam os direitos das crianças e jovens ao acesso à informação, liberdade de expressão, participação, educação e cultura.

Boa prática: Políticas e design adequado à idade

A desenvolvedora de aplicativos [Toca Boca](#) produz brinquedos digitais do ponto de vista infantil. A [política de privacidade](#) da empresa é projetada para compartilhar quais informações a empresa coleta e como são usadas. A Toca Boca, Inc é membro do programa de certificação [PRIVO Kids Privacy Assured COPPA Safe Harbor](#).

[LEGO® Life](#) é um exemplo de plataforma de mídia social segura para crianças menores de 13 anos compartilharem suas criações com LEGO, se inspirarem e interagirem com segurança. Aqui não é solicitado que as crianças forneçam informações pessoais para que possam criar uma conta, o que só é possível com o endereço de e-mail de um dos pais ou responsáveis. O aplicativo cria uma oportunidade para crianças e famílias discutirem segurança e privacidade online em um ambiente positivo.

Exemplos de design adequado à idade incluem ofertas específicas de algumas das principais emissoras de serviço público para determinados grupos de idade: por exemplo, o ARD (Arbeitsgemeinschaft der öffentlich-rechtlichen Rundfunkanstalten der Bundesrepublik Deutschland - Das Erste) e ZDF (Zweites Deutsches Fernsehen) ambos da Alemanha escolhem seu público alvo apenas a partir dos 14 anos, oferecendo conteúdo customizado através do [canal](#) [onlinefunk.net](#). A BBC (British Broadcasting Corporation) [lançou](#) oCBeebies, voltado para crianças menores de 6 anos. O conteúdo do site é feito sob medida para as respectivas faixas etárias.

Boa prática: Políticas e tecnologia

O Twitter tem investido continuamente em tecnologia proprietária, o que tem contribuído para reduzir constantemente o onus da denúncia das pessoas¹. Especificamente, mais de 50 por cento dos Tweets, em comparação com 20 por cento em 2018, acompanhados pelo Twitter devido à sua natureza abusiva, são reportados de forma proativa usando tecnologia, em vez de depender de denúncias ao Twitter. A nova tecnologia é usada para lidar com as áreas de conteúdo da política de informações privadas, mídia confidencial, conduta odiosa, abuso e falsificação de identidade.

1 Twitter, "15th Transparency Report: Increase in proactive enforcement on accounts".

3.2 Desenvolvimento de processos padronizados para lidar com material de pornografia infantil

Em 2019, a IWF acionou 132.676 páginas da web confirmadas como contendo abuso sexual infantil¹³. Qualquer URL pode conter centenas, senão milhares, de imagens e vídeos. Das imagens acionadas pelo IWF, 45 por cento mostravam crianças com 10 anos ou menos; e 1.609 páginas da web exibiam crianças de 0–2 anos, das quais 71 por cento continham abuso sexual mais grave, como estupro e tortura sexual. Esses fatos perturbadores ressaltam a importância da ação colaborativa entre a indústria, os governos, as autoridades policiais e a sociedade civil para combater a material de pornografia infantil.

Enquanto muitos governos estão enfrentando a disseminação e distribuição de CSAM promulgando legislação, investigando e processando abusadores, aumentando a conscientização e apoiando crianças e jovens na recuperação do abuso ou exploração, há muitos países que ainda não têm sistemas adequados em vigor. São necessários mecanismos em cada país para permitir que o público em geral denuncie conteúdo abusivo e exploratório dessa natureza. A indústria, a aplicação da lei, os governos e a sociedade civil devem trabalhar juntos para garantir a implementação de estruturas jurídicas adequadas de acordo com os padrões internacionais. Essas estruturas devem criminalizar todas as formas de CSEA, inclusive por meio de CSAM, e proteger as crianças vítimas de tal abuso ou exploração. Essas estruturas devem garantir que os processos de denúncias, investigações e remoção de conteúdo funcionem da forma mais eficiente possível.

A indústria deve fornecer links para linhas diretas nacionais ou outras linhas diretas disponíveis localmente, como os portais da IWF em alguns países e, na ausência de oportunidades para denunciar de forma local, fornecer links para outras linhas diretas internacionais conforme relevante, como o [Centro Nacional dos Estados Unidos para Crianças Desaparecidas e Exploradas](#) (NCMEC- *National Association of Internet Hotlines for Missing and Exploited Children*) ou a [Associação Internacional de Linhas Diretas da Internet](#) (INHOPE- *International Association of Internet Hotlines*), onde qualquer uma das linhas diretas internacionais pode ser usada para registrar uma denúncia.

As empresas responsáveis estão tomando uma série de medidas para ajudar a evitar que suas redes e serviços sejam usados para disseminar material pornográfico infantil. Isso inclui a introdução de linguagem nos termos e condições ou códigos de conduta que proíbem

13 IWF, "The why. The how. The who. And the results. Annual Report 2019".

explicitamente tal conteúdo ou conduta;¹⁴ o desenvolvimento de processos robustos de notificação e remoção; e o trabalho para apoiar as linhas diretas nacionais.

Além disso, algumas empresas implantam medidas técnicas para evitar o uso indevido de seus serviços ou redes para o compartilhamento de material pornográfico infantil conhecido. Por exemplo, alguns provedores de serviço de Internet estão bloqueando o acesso a URLs confirmados por uma autoridade apropriada como contendo material pornográfico infantil se o site estiver hospedado em um país onde não existem processos para garantir que será rapidamente retirado. Outros estão implantando tecnologias de hash para detectar e remover automaticamente imagens de abuso sexual infantil que já são conhecidas pela polícia ou pelas linhas diretas. Os membros da indústria devem considerar e incorporar todos os serviços relevantes nas suas operações para prevenir a disseminação do abuso sexual infantil.

Os atores da indústria devem se comprometer a alocar recursos proporcionais e continuar a desenvolver e compartilhar soluções tecnológicas de código aberto para detectar e remover material pornográfico infantil.

Boa prática: Tecnologia

A **Microsoft** usa uma abordagem de quatro vertentes para promover o uso responsável e seguro da tecnologia, com foco na própria tecnologia, autogovernança, parcerias e educação e alcance ao consumidor. A Microsoft também incorporou recursos que ajudam a capacitar os indivíduos a gerenciar sua segurança online de forma mais eficiente. “Family Safety” é um desses recursos, que permite que pais e responsáveis monitorem o uso da Internet por seus filhos.

A Microsoft aplica políticas contra assédio em suas plataformas, e os usuários que abusam dessas regulamentações estão sujeitos ao encerramento da conta ou, no caso de violações mais graves, a medidas de aplicação da lei.

Microsoft PhotoDNA é uma ferramenta que cria hashes de imagens e as compara a um banco de dados de hashes já identificados e confirmados como material pornográfico infantil. Se der match, a imagem é bloqueada. Essa ferramenta permitiu que os provedores de conteúdo removessem milhões de fotografias ilegais da Internet; ajudou a condenar predadores sexuais de crianças; e, em alguns casos, ajudou a polícia a resgatar vítimas potenciais antes que fossem fisicamente feridas. A Microsoft está comprometida há muito tempo em proteger seus clientes do conteúdo ilegal em seus produtos e serviços, e aplicar a tecnologia que a empresa já criou para combater o aumento e proliferação de vídeos ilegais foi o próximo passo lógico. No entanto, esta ferramenta não emprega tecnologia de reconhecimento facial, nem pode identificar uma pessoa ou objeto na imagem. Apesar disso, com a invenção do PhotoDNA para Vídeo, as coisas tomaram um novo rumo. PhotoDNA para Vídeo divide um vídeo em quadros-chave e, essencialmente, cria hashes para essas capturas de tela. Da mesma forma que o PhotoDNA pode corresponder a uma imagem que foi alterada para evitar a detecção, o PhotoDNA para Vídeo localiza conteúdo de exploração sexual infantil que foi editado ou combinado em um vídeo que poderia parecer inofensivo.

¹⁴ Deve-se observar que a conduta inadequada do usuário não se limita ao material pornográfico infantil e que qualquer tipo de comportamento ou conteúdo inadequado deve ser tratado de forma adequada pela empresa. [Diretrizes para a indústria sobre Proteção Infantil Online](#)

Além disso, a Microsoft lançou recentemente uma nova ferramenta para identificar predadores infantis que aliciavam crianças para serem abusadas em bate-papos online. O Projeto Artemis, desenvolvido em colaboração com The Meet Group, Roblox, Kik e Thorn, baseia-se na tecnologia patenteada da Microsoft e será disponibilizado gratuitamente via Thorn para empresas de serviço online qualificadas que oferecem uma função de chat. O Projeto Artemis é uma ferramenta de tecnologia que ajuda a alertar os administradores quando a moderação é necessária em salas de chat. Com esta técnica de detecção de aliciamento, será possível identificar, abordar e relatar predadores que tentam atrair crianças para fins sexuais.

A **IWF** fornece uma gama de serviços aos membros da indústria para proteger seus usuários de entrar em contato com material pornográfico infantil. Alguns exemplos são:

- Uma lista de bloqueio de URL dinâmica e de alta qualidade em tempo real;
- Uma lista hash de conteúdo criminoso conhecido relacionado ao material pornográfico infantil;
- Uma lista de palavras-chave exclusiva de termos enigmáticos conhecidos por serem associados ao material pornográfico infantil;
- Uma lista de detalhes de nomes de domínio conhecidos por hospedar conteúdo de abuso sexual infantil para permitir a remoção rápida de domínios que hospedam conteúdo ilegal.

3.3 Criação de um ambiente online mais seguro e adequado à faixa etária

Poucas coisas na vida podem ser consideradas absolutamente seguras e livres de riscos o tempo todo. Mesmo em cidades onde o movimento do tráfego é altamente regulamentado e estritamente controlado, acidentes ainda acontecem. Da mesma forma, o ciberespaço apresenta riscos, especialmente para crianças e jovens. Crianças e jovens podem ser vistos como receptores, participantes e atores em seu ambiente online. Os riscos que eles enfrentam podem ser classificados em quatro áreas¹⁵

- *Conteúdo impróprio*- Crianças e jovens podem se deparar com conteúdo impróprio e ilegal enquanto procuram por outra coisa clicando em um link presumivelmente inofensivo
- contido em alguma mensagem instantânea, em um blog ou ao compartilhar arquivos. Eles também podem procurar e compartilhar material impróprio ou inadequado à idade. O que é considerado conteúdo prejudicial varia de país para país; os exemplos incluem conteúdo que promove o consumo de drogas, ódio racial, comportamento de risco, suicídio, anorexia ou violência.
- *Conduta inadequada* - Crianças e adultos podem usar a Internet para assediar ou mesmo explorar outras pessoas. Há casos em que crianças podem transmitir comentários ofensivos ou imagens embaraçosas ou podem roubar conteúdo ou infringir direitos autorais.
- *Contato impróprio* - Tanto adultos quanto jovens podem usar a Internet para procurar crianças ou outros jovens vulneráveis. Frequentemente, seu objetivo é convencer o alvo

15 Sonia Livingstone et al., "EU Kids Online: Final Report", London School of Economics, 2009.

de que desenvolveram um relacionamento significativo, mas o propósito subjacente é manipulador. Eles podem tentar persuadir a criança a praticar atos sexuais ou outros atos abusivos online, usando uma webcam ou outro dispositivo de gravação, ou tentar marcar um encontro pessoal e contato físico. Este processo é frequentemente denominado de “aliciamento”.

- *Riscos Comerciais* – Esta categoria se refere à riscos de privacidade de dados relacionados à riscos de privacidade bem como marketing digital. A segurança online é um desafio da comunidade e uma oportunidade para a indústria e os governos e a sociedade civil trabalhar em conjunto para estabelecer princípios e práticas de segurança. A indústria pode oferecer uma variedade de abordagens técnicas, ferramentas e serviços para pais e filhos e jovens, que em primeiro lugar devem criar produtos que são fáceis de usar, que tenham um design seguro e conteúdo apropriado à faixa etária, para vários usuários. Outras abordagens incluem ferramentas para desenvolver sistemas apropriadas de verificação de idade que respeitam o direito de privacidade e acesso das crianças, ou que colocam restrições no acesso de crianças ou jovens à conteúdo não apropriado à sua faixa etária, ou restringem o acesso à pessoas com as quais as crianças poderão entrar em contato quando estão online. Mais importante, os marcos que incluem “design seguro”¹⁶ e privacidade devem ser incorporados nos processos de inovação e design de produtos. A segurança das crianças e o seu uso responsável da tecnologia deve ser priorizado e não visto como menos importante.

Alguns programas permitem que os pais monitorem os textos e outras comunicações que seus filhos e jovens enviam e recebem. Se programas desse tipo forem usados, é importante que isso seja discutido abertamente com a criança, caso contrário, tal conduta pode ser percebida como “espionagem” e pode minar a confiança dentro da família.

As políticas de uso aceitável são uma forma das empresas estabelecerem que tipo de comportamento tanto de adultos quanto de crianças é incentivado, quais tipos de atividades não são aceitáveis e as consequências de quaisquer violações a essas políticas. Mecanismos de denúncia claros e transparentes devem ser disponibilizados para usuários que tenham dúvidas sobre conteúdo e comportamento. Além disso, as denúncias devem ser acompanhados de forma adequada, com fornecimento oportuno de informações sobre o status da denúncia. Embora as empresas possam variar a implementação de mecanismos de acompanhamento caso a caso, é essencial definir um prazo claro para as respostas, comunicar a decisão tomada em relação à denúncia e oferecer um método de acompanhamento se o usuário não estiver satisfeito com a resposta.

16 Comissão de eSafety, Safety by Design Overview, 2019.

Boa prática: Relatórios e denúncias

O Facebook, em um esforço para conter o assédio sexual em plataformas digitais, co-financiou o Projeto deSHAME com a União Europeia, uma colaboração entre Childnet, Save the Children, Kek Vonale e UCLan. Este projeto visa aumentar a denúncia de assédio sexual online entre menores e melhorar a cooperação multissetorial na prevenção e resposta a esse comportamento.

Como um dos objetivos principais do projeto é encorajar os usuários a relatar conteúdo que é perturbador ou impróprio, os Padrões da Comunidade do Facebook também são relevantes como diretrizes sobre o que é ou não permitido no Facebook. Eles também descrevem os tipos de usuários que estão proibidos de postar. O Facebook também criou recursos de segurança como o recurso "Você conhece esta pessoa?" ; uma "outra" caixa de entrada que coleta novas mensagens de pessoas que o usuário não conhece; e um pop-up que aparece no feed de notícias caso parecer que um menor está sendo contatado por um adulto que não conhece.

Os provedores de serviços e conteúdo online também podem descrever a natureza do conteúdo ou dos serviços que fornecem e a faixa etária pretendida. Essas descrições devem estar alinhadas com os padrões nacionais e internacionais preexistentes, regulamentos relevantes e conselhos sobre marketing e publicidade para crianças disponibilizados pelos órgãos de classificação apropriados. Esse processo se torna mais difícil, no entanto, com a crescente gama de serviços interativos que permitem a publicação de conteúdo gerado pelo usuário, por exemplo, por meio de painéis de mensagens, salas de bate-papo e serviços de redes sociais. Quando as empresas visam especificamente crianças e jovens, e quando os serviços são predominantemente voltados para o público mais jovem, as expectativas em termos de **conteúdo e segurança amigáveis, facilmente compreensíveis e acessíveis** serão muito maiores.

As empresas também são incentivadas a adotar os mais altos padrões de proteção da privacidade quando se trata de coletar, processar e armazenar dados de ou sobre crianças e jovens, pois crianças e jovens podem não ter maturidade para apreciar as consequências sociais e pessoais mais amplas de revelar ou concordar em compartilhar suas informações pessoais online, ou quando forem usar suas informações pessoais para fins comerciais. Os serviços direcionados ou com probabilidade de atrair um público maior de crianças e jovens devem considerar os riscos apresentados a eles pelo acesso ou coleta e uso de informações pessoais (incluindo informações de localização) e garantir que esses riscos sejam devidamente tratados e os usuários informados. Em particular, as empresas devem garantir que a linguagem e o estilo de quaisquer materiais ou comunicação usados para promover serviços, fornecer acesso a serviços ou pelos quais informações pessoais são acessadas, coletadas e utilizadas, auxilia na compreensão dos usuários e no gerenciamento de sua privacidade de forma clara e simples, explicando o que eles estão consentindo em uma linguagem clara e acessível.

Boa prática: Inovação

Em 2018–2019, o Escritório Regional do UNICEF para o Leste da Ásia e Pacífico organizou cinco mesas redondas com várias partes interessadas para compartilhar práticas promissoras da indústria em abordar o abuso e exploração de crianças online. Os participantes das mesas redondas foram empresas líderes do setor privado, como Google, Facebook, Microsoft, Telenor, Ericsson, MobiCom (Mongólia) Mobifone + (Vietnã), Globe Telecom (Filipinas), True (Tailândia), GSMA e parceiros da sociedade civil, incluindo INHOPE, ECPAT International e Child Helpline International (Linhas Diretas para apoio Infantil Internacional).

Como parte do mesmo projeto, em fevereiro de 2020, o UNICEF lançou um Think Tank para acelerar a liderança da indústria na região do Leste Asiático e Pacífico na prevenção da violência contra crianças no mundo online. O Think Tank é uma incubadora de ideias e inovação, com base na perspectiva única dos atores da indústria (criação de produto, marketing, etc.) para o desenvolvimento de materiais educacionais impactantes e identificação das plataformas de entrega mais eficazes, bem como para o desenvolvimento de uma estrutura de avaliação que pode medir o impacto desses materiais educacionais e mensagens direcionadas às crianças. O Think Tank é composto pelo Facebook, Telenor, especialistas acadêmicos, agências das Nações Unidas, como a UIT, UNESCO e UNODC, e outros, como o Australia eSafety Commissioner, ECPAT International, ICMEC, INTERPOL e End Violence Global Fund (*Fundo Global para Acabar com a Violência*). A reunião inaugural do Think Tank, realizada paralelamente à Conferência Regional da ASEAN sobre Proteção Infantil Online, reuniu especialistas, incluindo a Microsoft, para explorar tecnologias e possibilidades de pesquisa para melhor rastrear mudanças no comportamento online, com base na aceitação de mensagens e materiais de segurança online.

3.4 Educar crianças, responsáveis e educadores sobre a segurança das crianças e o uso responsável das TICs

As medidas técnicas podem ser uma parte importante para garantir que as crianças e os jovens estão protegidos dos riscos potenciais online, mas são apenas um elemento da equação. Ferramentas de controle dos pais, conscientização e educação também são componentes-chave que ajudarão a capacitar e informar crianças e jovens de todas as idades, bem como pais, cuidadores e educadores. Embora as empresas tenham um papel importante em incentivar crianças e jovens a usar as TICs de forma responsável e segura, essa responsabilidade é compartilhada com pais, escolas, crianças e jovens.

Muitas empresas estão investindo em programas educacionais projetados para permitir que os usuários tomem decisões informadas sobre conteúdo e serviços. As empresas estão ajudando pais, responsáveis e educadores a orientar crianças e jovens para que tenham experiências on-line e em dispositivos móveis mais seguras, responsáveis e adequadas. Isso inclui a postagem de conteúdo sensível à idade e a garantia de que as informações sobre itens, como preços de conteúdo, termos de assinatura e como cancelar assinaturas, sejam comunicadas claramente. Promover o respeito ao requisito de idade mínima pelas redes sociais em todos os países onde a verificação da idade é possível também ajudaria a proteger as crianças, permitindo-lhes ter acesso aos serviços apropriados a sua idade. Uma consideração importante que deve acompanhar esta recomendação é a coleta de

dados pessoais adicionais que isso pode acarretar e a necessidade de limitar a coleta e o armazenamento dessas informações assim como seu processamento.

Também é importante fornecer informações diretamente a crianças e jovens sobre o uso mais seguro das TIC e sobre como ter um comportamento positivo e responsável. Além de aumentar a conscientização sobre segurança, as empresas podem facilitar experiências positivas desenvolvendo conteúdo para crianças e jovens sobre como podem ser respeitosos, gentis e ter a mente aberta ao usarem as TICs e cuidar dos amigos. Eles podem fornecer informações sobre as ações a serem tomadas se tiverem experiências negativas, como bullying ou aliciamento online, tornando mais fácil relatar tais incidentes e fornecendo uma função para cancelar o recebimento de mensagens anônimas.

Às vezes, os pais têm menos compreensão e conhecimento da Internet e de dispositivos móveis do que crianças e jovens. Além disso, a convergência de dispositivos móveis e serviços de Internet torna a supervisão dos pais mais difícil. A indústria pode trabalhar em colaboração com o governo e educadores para fortalecer a capacidade dos pais apoiarem seus filhos na construção de sua resiliência digital e na atuação como cidadãos digitais responsáveis. O objetivo não é transferir a responsabilidade pelo uso das TICs por crianças e jovens apenas para os pais, mas sim reconhecer que os pais estão em melhor posição para decidir o que é apropriado para seus filhos e que eles devem estar cientes de todos os riscos a fim de proteger melhor seus filhos e capacitá-los a agir.

As informações podem ser transmitidas online e offline por meio de múltiplos canais de mídia, levando em consideração que alguns pais não utilizam serviços de Internet. É importante colaborar com os distritos escolares para fornecer currículos sobre segurança online e uso responsável das TIC por crianças e jovens, e materiais educacionais para os pais. Os exemplos incluem explicar os tipos de serviços e opções disponíveis para atividades de monitoramento, ações a serem tomadas se uma criança estiver enfrentando bullying ou aliciamento online, como evitar spam e gerenciar configurações de privacidade e como falar com meninos e meninas de diferentes idades sobre assuntos delicados e problemas. A comunicação é um processo bidirecional e muitas empresas oferecem opções para os clientes contatá-los para relatar problemas ou discutir preocupações.

À medida que o conteúdo e os serviços ficam cada vez mais ricos, todos os usuários continuarão a se beneficiar de conselhos e lembretes sobre a natureza de um serviço específico e como aproveitá-lo com segurança. Embora seja importante ensinar as crianças sobre o uso responsável da Internet, sabemos que as crianças gostam de experimentar, correr riscos, são intrinsicamente curiosas e nem sempre tomam as melhores decisões. Dar a eles a chance de exercer seu arbítrio contribui para seu crescimento e é uma maneira saudável de ajudá-los a desenvolver autonomia e resiliência, desde que a reação não seja muito dura. Embora as crianças devam ser permitidas a correr alguns riscos no ambiente online, é fundamental que os pais e as empresas possam apoiá-las quando as coisas dão errado, pois isso pode compensar o impacto negativo de uma experiência desconfortável e transformá-la em uma lição útil para o futuro.

Boa prática: Educação

NHK Japan realiza uma [campanha de prevenção de suicídio](#) para jovens no Twitter: No Japão, os suicídios entre adolescentes atingem o pico quando eles voltam para a escola após as férias de verão. O retorno à realidade é considerado a razão do pico. A equipe de produção da NHK Heart Net TV (NHK Japan) produz um programa multimídia [#Na noite de 31 de agosto](#) (#OnTheNightOfAugust21st). Conectando televisão, transmissão ao vivo e mídia social, a NKH criou com sucesso um “lugar” onde os adolescentes podiam compartilhar seus sentimentos sem medo.

O Twitter também publicou um [guia para educadores sobre alfabetização midiática](#). Elaborado com a UNESCO, o manual tem como objetivo principal ajudar os educadores a equipar as gerações mais jovens com habilidades de alfabetização midiática. Outro aspecto do trabalho de segurança do Twitter está relacionado à [divulgação das operações de informações](#). Este é um arquivo de operações de informações apoiadas pelo Estado, que o Twitter compartilha publicamente. A iniciativa foi lançada para capacitar a compreensão acadêmica e pública das campanhas relacionadas a esse problema em todo o mundo e para capacitar o escrutínio independente de terceiros dessas táticas na plataforma do Twitter.

O Projeto deSHAME, co-financiado pelo Facebook e pela União Europeia, também facilita a criação de recursos para uma ampla gama de grupos de idade, com foco particular em crianças de 9 a 13 anos. Como parte do projeto, um kit de ferramentas chamado [“Step Up, Speak Up!”](#) (Tome um passo, Fale!) foi desenvolvido, fornecendo uma variedade de materiais de educação, treinamento e conscientização, bem como ferramentas práticas para prevenção multissetorial e estratégias de resposta. O projeto irá transferir esses materiais de aprendizagem para outros países europeus e parceiros em todo o mundo, a fim de promover os direitos digitais dos jovens.

Boa prática: Educação

A Google desenvolveu uma série de iniciativas, recursos e ferramentas educacionais para ajudar a promover a segurança online para jovens. Uma delas é a campanha Seja Incrível na Internet ([Be Internet Awesome](#)) em torno da cidadania digital, criada em colaboração com organizações como a Se Conecte Seguro (*ConnectSafely*), o Instituto de Segurança Online da Família (*Family Online Safety Institute*) e a Coalizão de Segurança Online (Internet Keep Safe Coalition). Esta campanha é direcionada a jovens de 8-11 anos. Ela apresenta um jogo baseado na web para jovens (Interland) que ensina fundamentos e recursos de segurança digital para educadores, como Cidadania Digital e Currículo de Segurança. O Currículo de Segurança oferece planos de aula para as cinco áreas temáticas principais da campanha, uma das quais enfoca o cyberbullying. Além disso, o Google gerou um curso online de cidadania digital e segurança para educadores de alunos de todas as idades, fornecendo suporte adicional para a integração da cidadania digital e atividades de segurança na sala de aula. O Google também oferece vários programas para ajudar a envolver os jovens diretamente nos esforços de segurança on-line e cidadania digital. A iniciativa global Web Rangers é um programa que ensina os jovens sobre segurança online e os incentiva a projetar suas próprias campanhas em torno do uso positivo e seguro da Internet. Existem também programas específicos de cada país para jovens, como os programas Internet Citizens (Cidadãos da Internet) e Internet Legends (Heróis da Internet) no Reino Unido, lançados pelo Google.

No **Eurovision Youth News Exchange**, a União de Emissoras Europeias (*European Broadcasting Union*) reúne 15 emissoras de televisão europeias para compartilhar programas, formatos e soluções online e offline. Nos últimos anos, o ensino da alfabetização digital e o alerta às crianças sobre os riscos na Internet se tornaram fundamentais para seus programas. Entre as iniciativas mais bem-sucedidas dos últimos anos estão os anúncios de mídia social e programas de notícias adequados para crianças produzidos por Super e Ultra nytt sob a NRK, a emissora pública da Noruega.

Boa prática: Parcerias estratégicas

Como parte de um projeto apoiado pelo [Fundo para Acabar com a Violência contra a Criança](#), (*End Violence Against Children Fund*) em 2018 a [Capital Humano y Social Alternativo](#) firmou uma parceria com a Telefónica, a maior operadora de Internet, cabo e telefone do Peru, com 14,4 milhões de clientes, incluindo mais de 8 milhões Usuários móveis da Movistar.

Várias atividades foram realizadas no âmbito desta parceria frutífera:

- Um curso virtual sobre proteção infantil online foi desenvolvido pela Telefónica com o apoio técnico de Capital Humano y Social Alternativo. Este curso está agora disponível abertamente no site da Telefónica e a empresa está monitorando o número de pessoas que se inscrevem e concluem o curso com sucesso. O Ministério da Educação do Peru concordou em incluir o acesso a este curso virtual por meio de seu site oficial.
- Um livreto sobre segurança na Internet foi elaborado pela Capital Humano y Social Alternativo e distribuído pela Telefónica em seus mais de 300 centros de vendas móveis. O objetivo é conscientizar os clientes da Telefónica sobre a segurança online e os riscos associados ao abuso e exploração de crianças online.
- Um jogo interativo sobre abuso e exploração de crianças online foi desenvolvido pela Telefónica com o apoio técnico de Capital Humano y Social Alternativo, que seus clientes podem jogar enquanto aguardam sua vez para serem atendidos nas lojas da Telefónica.

Com base no sucesso da Telefónica, a Capital Humano y Social Alternativo fez parceria com a Econocable, uma provedora de serviços de Internet e cabo que atua em áreas remotas e de baixa renda no Peru.

3.5 Promover a tecnologia digital como um meio para aumentar o engajamento cívico

O artigo 13 da Convenção das Nações Unidas sobre os Direitos da Criança afirma que "a criança tem direito à liberdade de expressão; este direito deve incluir a liberdade de buscar, receber e transmitir informações e idéias de todos os tipos, independentemente de fronteiras, seja oralmente, por escrito ou por impressão, na forma de arte, ou por qualquer outro meio de escolha da criança." As empresas podem cumprir seu dever de respeitar os direitos civis e políticos de crianças e jovens, garantindo que a tecnologia e a aplicação de legislação e políticas desenvolvidas para proteger crianças e jovens de danos on-line não tenham as consequências indesejadas de suprimir seu direito de participação e expressão ou impedindo-os de acessar informações importantes para o seu bem-estar. É essencial garantir que os sistemas de verificação de idade não coloquem em risco a necessidade genuína de grupos de idade específicos acessarem conteúdos que sejam relevantes para o seu desenvolvimento.

Ao mesmo tempo, as empresas e as indústrias também podem apoiar os direitos das crianças e dos jovens, fornecendo mecanismos e ferramentas para facilitar a participação dos jovens. Eles podem enfatizar a capacidade da Internet de facilitar o envolvimento positivo na vida cívica mais ampla, impulsionar o progresso social e influenciar a sustentabilidade e a resiliência das comunidades, por exemplo, participando de campanhas sociais e ambientais

e responsabilizando os responsáveis. Com as ferramentas e informações certas, crianças e jovens estarão melhor posicionados para ter acesso a oportunidades de assistência médica, educação e emprego, e para expressar suas opiniões e necessidades nas escolas, comunidades e países. Eles adquirem o poder de acessar informações sobre seus direitos e buscar informações sobre questões que os afetam pessoalmente, como sua saúde sexual e sobre a responsabilidade política e governamental.

As empresas também podem investir na criação de experiências online adequadas para crianças, jovens e famílias. Eles podem apoiar o desenvolvimento de tecnologia e conteúdo que incentive e capacite crianças e jovens a aprender, inovar e criar soluções. Devem sempre considerar a segurança desde o projeto de seus produtos.

Além disso, as empresas podem apoiar de forma proativa os direitos das crianças e dos jovens, trabalhando para eliminar a exclusão digital. A participação de crianças e jovens requer alfabetização digital - a capacidade de compreender e interagir no mundo digital. Sem essa capacidade, os cidadãos não podem participar de muitas das funções sociais que foram digitalizadas, incluindo declaração de impostos, apoio a candidatos políticos, assinatura de petições online, registro de nascimento ou simplesmente acesso a informações comerciais, de saúde, educacionais ou culturais. Sem ação, o fosso entre os cidadãos que têm acesso a esses fóruns e os que não têm, por falta de acesso à Internet ou alfabetização digital, continuará a aumentar, colocando estes últimos em significativa desvantagem. As empresas podem apoiar iniciativas de multimídia para promover as habilidades digitais que crianças e jovens precisam para serem cidadãos confiantes, conectados e ativamente envolvidos.¹⁷ Em muitos países, a alfabetização digital e midiática e os esforços para eliminar a exclusão digital têm feito parte da missão da mídia de serviço público nos últimos anos. O Parlamento italiano, por exemplo, propôs que as prioridades da emissora nacional incluíssem o fim da exclusão digital e a garantia da proteção da criança tanto offline quanto online, um exemplo que poderia ser seguido por outros países.

Boa prática: Colaboração entre as agências

Recentemente, a Microsoft aderiu à campanha global Poder do ZERO ([Power of ZERO](#)), liderada pela organização No Bully, que visa ajudar as crianças e os adultos que cuidam delas a aprender a usar bem a tecnologia digital e a desenvolver a voz, a compaixão e a inclusão que são o coração da cidadania digital. A iniciativa oferece aos primeiros educadores (a campanha é direcionada a crianças de 8 anos ou menos) e famílias materiais de aprendizagem gratuitos para ajudar as crianças a cultivar os "12 poderes para o bem" (habilidades de vida dos 12 Poderes do Zero ou "poderes", para crianças navegarem com sucesso no mundo online e offline, incluindo resiliência, respeito, inclusão e criatividade) e estabelecer uma base sólida para eles em uma idade precoce.

17 Para ver exemplos de participação de jovens na comunidade móvel, [clique aqui](#).

4 Diretrizes gerais para a indústria

A Tabela 1 descreve as diretrizes gerais para a indústria identificar, prevenir e mitigar quaisquer impactos adversos de produtos e serviços sobre os direitos das crianças e jovens e para promover o uso positivo das TICs por crianças e jovens.

Observe que nem todas as etapas listadas na Tabela 1 serão adequadas para todas as empresas e serviços, e nem todas as etapas necessárias para cada serviço estão nesta Tabela. As diretrizes gerais para a indústria são complementadas pelas listas de verificação de recursos específicos (consulte a seção 5) e vice-versa. As listas de verificação específicas de recursos nas Tabelas 2-5 destacam etapas adicionais que são mais relevantes para serviços individuais. Observe que as listas de verificação específica aos recursos podem se sobrepor e que mais de uma lista de verificação pode ser relevante para o mesmo serviço.

Tabela 1: Diretrizes gerais para a indústria

Integrar os direitos da criança em todas as políticas corporativas e processos de gestão adequados	A indústria pode identificar, prevenir e mitigar os impactos adversos das TICs nos direitos das crianças e dos jovens e identificar oportunidades para apoiar o avanço dos direitos das crianças e dos jovens, tomando as seguintes ações:
	Certificar que uma pessoa e/ou equipe específica seja designada como responsável por esse processo e tenha acesso às partes interessadas internas e externas necessárias. Autorize essa pessoa ou equipe a assumir a liderança na promoção da proteção infantil online em toda a empresa.
	Desenvolver uma política de proteção e salvaguarda da criança e/ou integrar riscos e oportunidades específicas relativas aos direitos das crianças e dos jovens nos compromissos das políticas de toda a empresa (por exemplo, direitos humanos, privacidade, marketing e códigos de conduta relevantes).
	Integrar a devida diligência em questões de PIO aos direitos humanos existentes ou estruturas de avaliação de risco (no nível corporativo, de produto ou tecnologia e/ou de país) para determinar se o negócio ou indústria pode estar causando ou contribuindo para impactos adversos através de suas atividades, ou se os impactos adversos podem ser atribuídos diretamente às suas operações, produtos ou serviços, ou relações comerciais.
	Identificar os impactos dos direitos da criança em diferentes grupos etários como resultado das operações da empresa e do design, desenvolvimento e introdução de produtos e serviços, bem como oportunidades de apoiar os direitos das crianças e jovens.

Integração das considerações com os direitos das crianças em todas as políticas corporativas apropriadas e processos de gestão (cont.)	Adote uma abordagem baseada na capacitação e na educação em relação à proteção da criança. Considere os direitos de proteção de dados das crianças, seu direito à privacidade e à liberdade de expressão, oferecendo educação e apropriada através dos serviços da empresa. Aproveitar a experiência interna e externa e consulte os principais parceiros, incluindo crianças e jovens, sobre mecanismos de segurança online para obter feedback contínuo e orientação sobre as abordagens da empresa.
	Em Estados que carecem de marcos jurídicos adequados para a proteção dos direitos das crianças e jovens à privacidade e à liberdade de expressão, as empresas devem garantir que as políticas e práticas estejam alinhadas as normas Internacionais. Veja Resolução 68/167 da Assembleia Geral da ONU sobre o direito à privacidade na era digital. Garantir o acesso à remediação, estabelecendo mecanismos operacionais de denúncia e reclamação sobre quaisquer violações dos direitos da criança (por exemplo, CSAM, conteúdo ou contato impróprio ou violação de privacidade). Nomear um gerente de políticas de proteção à criança ou outra pessoa designada que possa ser contatada para questões de PIO. Se uma criança corre o risco de se machucar, o gerente da política de proteção infantil deve alertar imediatamente as autoridades competentes. Nas Diretrizes editoriais da BBC (2019, BCC Editorial Guidelines), por exemplo, especifique a nomeação de um gestor para a política de proteção infantil, que é obrigatório dentro do âmbito de serviço social público.
Desenvolvendo padrões da indústria para proteger as crianças online	Criar e implementar padrões empresariais e da indústria para a proteção de crianças e jovens, no que diz respeito às especificidades da indústria e dos recursos.
Desenvolvendo processos padrão-Para material de pornografia infantil (CSAM)	Em colaboração com o governo, agentes policiais, sociedade civil e organizações de linha direta, a indústria tem um papel fundamental a desempenhar no combate de material de pornografia infantil online:
	Proibir upload, postagem, transmissão, compartilhamento ou a disponibilização de conteúdo que viole os direitos de qualquer parte ou infrinja qualquer lei local, estadual, nacional ou internacional. Comunicar com as agências nacionais de aplicação da lei ou com as linhas diretas para comunicar denúncias de CSAM assim que estes forem trazidos ao conhecimento do provedor. Certificar que procedimentos internos estejam em vigor para cumprir as responsabilidades de relatar de acordo com as leis locais e internacionais. Quando uma empresa opera em mercados onde a supervisão regulatória e aplicação da lei sobre este assunto são menos desenvolvidos, pode referir aqueles que desejam denunciar à Associação Internacional de Linhas Diretas da Internet (INHOPE), onde os relatórios podem ser arquivados com qualquer linha direta.

Desenvolvendo processos padrão Para material pornográfico Infantil (CSAM) (cont.)

Estabelecer procedimentos internos para garantir a conformidade com as normas locais e leis internacionais de combate ao CSAM.

Estabelecer um cargo sênior ou equipe dedicada a integrar esses procedimentos na organização. Os membros da indústria devem então relatar as ações tomadas e os resultados alcançados por esta equipe em seus relatórios anuais corporativos de sustentabilidade.

Quando os regulamentos nacionais não fornecem proteção suficiente, as empresas devem respeitar, mas exceder a legislação nacional e usar seu poder para fazer lobby por mudanças legislativas que permitam que a indústria combata CSAM.

Um cargo sênior ou equipe deve ser criado dentro da organização, dedicado a integrar esses procedimentos e monitorar as operações. Estes devem ser refletidos de forma transparente nos relatórios corporativos e de sustentabilidade anuais disponibilizados ao público.

Especificar que a empresa irá cooperar totalmente com as investigações policiais no caso de conteúdo ilegal ser denunciado ou descoberto e observar detalhes sobre penalidades como multas ou cancelamento de privilégios de faturamento.

Usar os termos e condições do cliente e/ou políticas de uso aceitáveis para declarar explicitamente a posição da empresa sobre o uso indevido de seus serviços para armazenar ou compartilhar CSAM e as consequências de qualquer abuso.

Desenvolver processos de notificação, retirada e denúncia que permitam que usuários relatem CSAM ou contato impróprio e o perfil específico onde foi detectado.

Estabelecer processos de acompanhamento de denúncias, concordar com os procedimentos de coleta de evidências e imediatamente remover ou bloquear o acesso ao CSAM.

Certificar que, quando necessário, os prestadores de serviços solicitem a opinião de especialistas (por exemplo, órgãos nacionais da PIO) antes de destruir o conteúdo ilegal.

Garantir que terceiros relevantes com os quais a empresa tenha uma relação contratual tenham também processos de notificação e remoção robustos em vigor.

Esteja preparado para lidar com o CSAM e relatar casos às autoridades competentes. Se uma relação com as autoridades policiais e as linhas diretas nacionais ainda não foi estabelecida, envolva-se com eles para desenvolver processos conjuntamente.

Trabalhar com funções internas, como atendimento ao cliente, prevenção de fraude e segurança para garantir que a empresa possa enviar relatórios de suspeita de conteúdo ilegal diretamente para as autoridades policiais e linhas diretas.

Idealmente, isso deve ser feito de uma forma que não exponha profissionais da linha de frente a conteúdo prejudicial nem vitimize novamente a criança/crianças e jovens afetados. Para lidar com situações onde a equipe pode ser exposta a materiais abusivos, implementar uma política ou programa para apoiar a resiliência, segurança e bem-estar da equipe.

Desenvolvendo processos padronizados para material pornográfico infantil (CSAM)	Incluir políticas de retenção e preservação de dados para apoiar a execução da aplicação atividades como a coleta de evidências. Documente as práticas da empresa que lidam com material pornográfico infantil, começando com o monitoramento e se estendendo até a transferência e destruição do conteúdo. Inclua uma lista de todo o pessoal responsável pelo manuseio do material na documentação.
(cont.)	Promover mecanismos de denúncia de material pornográfico infantil e garanta que os clientes saibam como registrar uma denúncia se descobrirem tal conteúdo. Caso houver uma linha direta nacional disponível, ofereça links para essa linha direta no site corporativo e em quaisquer serviços de conteúdo relevantes promovidos pela empresa.
	Usar todos os serviços/conjuntos de dados relevantes para evitar a disseminação de conteúdo conhecido de abuso sexual infantil em seus serviços ou plataformas.
	Avaliar ativamente todo o conteúdo hospedado nos servidores da empresa, incluindo comercial (de marca ou contratado de provedores de conteúdo de terceiros) regularmente. Considere o uso de ferramentas como verificação de hash de imagens conhecidas de abuso sexual infantil, software de reconhecimento de imagem ou bloqueio de URL para lidar com material pornográfico infantil.
Criando um ambiente online mais seguro e apropriado à faixa etária	A indústria pode ajudar a criar um ambiente digital mais seguro e agradável para crianças e jovens de todas as idades, realizando as seguintes ações:
	Adotar os princípios de segurança e design de privacidade na empresa assim como tecnologias e serviços e priorizar soluções que reduzam o volume mínimo de dados relativos às crianças.
	Implementar designs adequados à idade nos serviços oferecidos.
	Apresentar informações às crianças sobre as regras do site em um formato acessível e apropriado para a idade, fornecendo a quantidade certa de detalhes.
	Além de termos e condições que sejam adequados e acessíveis à idade, a indústria deve da mesma forma claramente comunicar informações, como regras e políticas-chave. Isso deve enfatizar quais comportamentos são aceitáveis e inaceitáveis ao usar o serviço, as consequências de quebrar quaisquer regras, as especificações do serviço e com o que o usuário concorda ao se inscrever. Estas informações, devem ser especialmente voltadas para usuários jovens, seus pais e cuidadores.
	Use os termos de serviço ou termos e condições para chamar a atenção dos usuários para conteúdo nos serviços online da empresa que podem não ser apropriados para todas as idades. Os termos e condições também devem incluir mecanismos para denunciar e lidar com as infrações a essas regras.

Criando um Ambiente online mais seguro e apropriado à faixa etária (cont.)

Considerar fornecer mecanismos como software de controle parental e outras ferramentas que permitem que pais e responsáveis gerenciem o acesso de seus filhos a recursos da Internet enquanto fornecem orientação sobre o uso apropriado para que os direitos das crianças não sejam infringidos. Estes devem incluir listas de bloqueio/aceitação, filtros de conteúdo, monitoramento de uso, gestão de contato e limites de tempo/programa.

Oferecer opções de controle parental fáceis de usar que permitem aos pais e cuidadores restringir certos serviços e conteúdos que as crianças podem acessar ao usar dispositivos eletrônicos. Essas restrições podem incluir controles de rede e de dispositivos e controles de aplicativos. Considerando que isso tem uma grande implicação na capacidade de uma criança melhorar suas habilidades digitais ou prejudicar suas oportunidades online, esses controles devem ser projetados para crianças muito pequenas, de acordo com o seu contexto de desenvolvimento e com orientação adequada para os pais.

Sempre que possível, promova serviços nacionais de apoio que os pais e os cuidadores podem usar para relatar infrações e buscar apoio em casos de abuso ou exploração.

Evitar conteúdo publicitário prejudicial ou impróprio online e estabeleça obrigações de divulgação do cliente para provedores de serviços com conteúdo que destina-se ao público adulto e pode ser prejudicial a crianças e jovens. Publicidade prejudicial também pode incluir publicidade sobre alimentos e bebidas com alto teor de gordura, açúcar ou sal.

Alinhar as práticas de negócios com regulamentos e conselhos sobre marketing e publicidade para crianças e jovens. Monitorar onde, quando e como crianças e jovens se deparam com mensagens publicitárias destinadas a outro segmento de mercado e potencialmente prejudiciais.

Certificar que as políticas de coleta de dados estejam em conformidade com as leis relevantes em relação à privacidade de crianças e jovens, incluindo a consideração sobre se o consentimento parental é necessário antes que empresas comerciais possam coletar informações pessoais de ou sobre uma criança.

Adaptar e implementar configurações mais rigorosas de privacidade para a coleta, processamento, armazenamento, venda e publicação de dados pessoais, incluindo informações relacionadas à localização e hábitos de navegação, coletados de menores de 18 anos. Configurações e informações de privacidade sobre a importância da privacidade devem ser adequadas à idade dos usuários e a natureza do serviço.

Empregar medidas técnicas, como ferramentas adequadas de controle parental, design de segurança, experiências diferenciadas por idade, conteúdo protegido por senha, listas de bloqueio/permissão, controles de compra/tempo, funções de desativação, filtragem e moderação, para evitar o acesso e a exposição de menores de idade a conteúdo ou serviços inadequados. Implementar tecnologia que possa identificar a idade dos usuários e apresentá-los com uma versão do aplicativo apropriada à sua idade.

Para conteúdo ou serviços sensíveis à idade, as partes interessadas da indústria devem tomar medidas para verificar a idade dos usuários. Se possível: usar verificação de idade para limitar o acesso a conteúdo ou material que, por lei ou política, destina-se apenas a pessoas acima de uma certa idade.

As empresas também devem reconhecer o potencial de uso indevido de tais tecnologias para restringir o direito de crianças e jovens à liberdade de expressão e acesso à informação ou colocar em risco a sua privacidade.

Criação de um ambiente online mais seguro e apropriado à faixa etária

(cont.)

Certificar que o conteúdo e os serviços que não são apropriados para usuários de todas as idades sejam:

- classificados de acordo com os padrões nacionais e normas culturais;
- consistentes com os padrões existentes em meios equivalentes;
- identificados com opções de exibição proeminentes para controlar o acesso;
- oferecidos junto com a verificação de idade, quando possível apropriado e com termos claros relacionados ao apagamento de quaisquer dados pessoalmente identificáveis obtidos através do processo de verificação.

Por exemplo, com relação aos padrões de mídia, todas as autoridades regulatórias de mídia fornecem um conjunto de requisitos para conteúdo relacionado à idade e os provedores de Internet são obrigados a adaptar os repositórios e aplicar as diretrizes à sua oferta de conteúdo. Veja [Ofcom no Reino Unido](#), [CSA na França](#) e [AGCOM na Itália](#).

Oferecer ferramentas de denúncia claras e desenvolva um processo de acompanhamento das denúncias de conteúdo impróprio, contato e uso indevido, e forneça feedback detalhado aos usuários do serviço sobre o processo da denúncia.

Assegurar a pré-moderação de espaços interativos projetados para crianças e jovens de forma congruente com os direitos das crianças à privacidade e suas capacidades em evolução. A moderação ativa pode encorajar um ambiente onde o bullying e o assédio não são aceitáveis. O comportamento inaceitável inclui:

- postar comentários desagradáveis ou ameaçadores no perfil de alguém;
- criação de perfis falsos ou sites de ódio para humilhar a vítima;
- enviar mensagens em cadeia e anexos com intenções prejudiciais;
- invadir a conta de alguém para enviar mensagens ofensivas a outras pessoas.

Tenha especial cuidado com os funcionários ou colaboradores que trabalham com crianças e jovens, para os quais pode ser necessária uma verificação prévia do registro criminal junto das autoridades policiais.

Encaminhar qualquer incidente de suspeita de aliciamento imediatamente à equipe de gerenciamento executivo online ou interativo responsável por relatá-lo às autoridades competentes:

- denuncie aliciamento para a equipe de gestão executiva e para um gerente de política de proteção infantil nomeado, sempre que possível;
- permita que os usuários relatem incidentes de aliciamento diretamente às autoridades;
- estabeleça a possibilidade de contato direto através de endereços de e-mail para alertar e denunciar.

Priorize a segurança e o bem-estar da criança em todos os momentos. Aja sempre dentro dos limites profissionais e garanta que todo contato com crianças seja essencial para o serviço, programa, evento, atividade ou projeto. Nunca assuma a responsabilidade exclusiva por uma criança. Se uma criança precisar de cuidados, alerte os pais, responsáveis ou acompanhantes. Ouça e respeite as crianças em todos os momentos. Se alguém estiver se comportando de maneira inadequada com crianças, relate o comportamento ao contato local da proteção à criança.

Criando um ambiente mais seguro e apropriado à faixa etária (cont.)	Estabelecer um conjunto claro de regras que são colocadas de forma proeminente e que ecoem pontos dos termos de serviço e diretrizes de uso aceitável importantes. Linguagem apropriada ao usuário para essas regras deve definir: • a natureza do serviço e o que se espera de seus usuários; • o que é e não é aceitável em termos de conteúdo, comportamento e linguagem, bem como proibir o uso ilegal; • as consequências proporcionais à violação, por exemplo, denúncia à polícia ou suspensão da conta do usuário. Facilitar que os clientes relatem preocupações sobre o uso indevido ao atendimento ao cliente, com processos padronizados e acessíveis para lidar com preocupações diferentes, como receber comunicações indesejadas (por exemplo, SMS de spam). Seja transparente e forneça aos clientes informações claras sobre a natureza dos serviços oferecidos, por exemplo: • tipo de conteúdo/serviço e custos; • idade mínima exigida para acesso; • disponibilidade de controles dos pais, incluindo o que os controles cobrem (por exemplo, rede) ou não cobrem (por exemplo, Wi-Fi) e treinamento sobre como usá-los; • tipo de informação do usuário coletada e como ela é usada. Promover serviços de apoio nacional que capacitem crianças e jovens a denunciar e buscar apoio em caso de abuso ou exploração (ver, por exemplo, Child Helpline International).
Educar filhos, pais e educadores sobre a segurança das crianças e seu uso responsável de TICs.	A indústria pode complementar medidas técnicas com medidas educacionais e atividades de capacitação, tomando as seguintes ações: Descrever claramente o conteúdo disponível e os controles parentais correspondentes ou configurações de segurança familiar. Torne a linguagem e a terminologia acessível, visível, clara e relevante para todos os usuários, incluindo crianças, pais e cuidadores, especialmente em relação aos termos e condições, custos envolvidos no uso de conteúdo ou serviços, políticas de privacidade, informações de segurança e mecanismos de denúncia. Educar os clientes sobre como gerenciar questões relacionadas ao uso da Internet, incluindo spam, roubo de dados e contato impróprio, como bullying e aliciamento, e descrever quais ações os clientes podem tomar e como eles podem levantar questões sobre o uso impróprio. Estabelecer mecanismos e educar os pais a se envolverem nas atividades de uso de TICs de seus filhos e jovens, particularmente as de crianças mais novas, por exemplo, permitindo que os pais avaliem as configurações de privacidade dos jovens e crianças. Colaborar com o governo e educadores para elaborar as habilidades de pais apoiarem e conversarem com seus filhos e jovens sobre ser cidadãos digitais e usuários responsáveis de TICs. Com base no contexto local, fornecer materiais educacionais para serem usadas em escolas e lares para melhorar o uso que crianças e jovens fazem das TICs e desenvolver o pensamento crítico para permitir que eles se comportem com segurança e de forma responsável ao usar os serviços de TIC.

Educar filhos, pais e educadores sobre a segurança das crianças e seu uso responsável de TICs. (cont.)	Oferecer suporte aos clientes, disseminando diretrizes sobre segurança online familiar que incentivam os pais e cuidadores a: • familiarizar-se com os produtos e serviços usados por crianças e jovens; • garantir o uso moderado de dispositivos eletrônicos por crianças e jovens como parte de um estilo de vida saudável e equilibrado; • prestar muita atenção ao comportamento das crianças e jovens a fim de identificar mudanças que possam indicar cyberbullying ou assédio.
Usando avanços tecnológicos para proteger e educar crianças	IA que preserva a privacidade, entende textos, imagens, conversas e contextos, pode detectar e abordar uma série de danos online e ameaças e usar essas informações para capacitar e educar as crianças para lidar com eles. Quando realizado dentro do ambiente do dispositivo inteligente, isso pode proteger os dados e a privacidade dos jovens enquanto ainda os apoia. O serviço público e a mídia nacional podem desempenhar um papel essencial por meio do oferecimento da sua programação (offline e online) para educar os pais e crianças e torná-los cientes dos riscos e oportunidades do universo online.
Promover a tecnologia como ferramenta para reforçar ainda mais o engajamento cívico	A indústria pode encorajar e capacitar crianças e jovens ao apoiar seu direito de participação por meio das seguintes ações: Fornecer informações sobre um serviço para destacar os benefícios que crianças obtêm comportando-se bem e com responsabilidade, como quando usam o serviço para fins criativos. Estabelecer procedimentos escritos que garantam a implementação consistente de políticas e processos que protegem a liberdade de expressão de todos os usuários, incluindo crianças e jovens, bem como a documentação de conformidade com essas políticas. Evitar o bloqueamento excessivo de conteúdo legítimo e apropriado para o desenvolvimento. A fim de garantir que as solicitações e ferramentas de filtragem não sejam usadas de modo a restringir o acesso de crianças e jovens à informação, e engajamento cívico garanta a transparência sobre o conteúdo bloqueado e estabeleça um processo para usuários relatarem o bloqueio inadvertido. Este processo deve estar disponível para todos os consumidores, incluindo webmasters. Qualquer processo de denúncia deve fornecer termos de serviço claros, responsáveis e adjudicados. Colaborar com a sociedade civil local e o governo nas prioridades nacionais e locais para expandir o acesso universal e equitativo às TICs, plataformas e dispositivos, e a infraestrutura subjacente para apoiá-los. Informar e envolver clientes, incluindo pais, cuidadores, crianças e jovens, sobre os serviços oferecidos, por exemplo: • tipo de conteúdo e controles parentais correspondentes; • mecanismos de denúncia de casos de abuso, uso indevido e conteúdo impróprio ou ilegal; • procedimentos de acompanhamento de denúncias; • tipos de serviços com restrição de idade; • uso seguro e responsável de serviços interativos de “marca própria”.

Promover a tecnologia como ferramenta para reforçar ainda mais o engajamento cívico (cont)	Se envolver com as questões mais amplas em torno da cidadania digital segura e responsável, por exemplo, reputação online e pegada digital, conteúdo prejudicial e aliciamento. Considere fazer parceria com especialistas locais, como ONGs infantis, instituições de caridade e grupos de pais, para ajudar a moldar a mensagem da empresa e atingir o público-alvo.
	Se a empresa já trabalha com crianças ou escolas, por exemplo, por meio de programas de responsabilidade social corporativa, investigar a possibilidade de estender este compromisso para incluir educação e engajamento com crianças e jovens, e educadores sobre mensagens PIO.
Investir em pesquisa	Invista em pesquisas baseadas em evidências e análises aprofundadas das tecnologias digitais, seu impacto nas crianças, proteção infantil e considerações sobre os direitos da criança em relação ao ambiente digital, para integrar sistemas de proteção online em serviços usados por crianças e jovens e melhor entender quais tipos de intervenções são mais eficazes para melhorar as experiências online das crianças.

Tipologia de empresas de TIC

Embora essas diretrizes da UIT sejam direcionadas à indústria de TIC como um todo, é importante reconhecer que os serviços que as empresas de TIC oferecem, as formas como operam, os esquemas regulatórios sob os quais funcionam e o escopo e a escala de suas ofertas diferem muito. Qualquer empresa de tecnologia cujos produtos e serviços são direcionados direta ou indiretamente para crianças pode se beneficiar dos princípios gerais descritos anteriormente e pode adaptá-los, com base em seu campo específico de operação. A ideia central é apoiar e orientar a indústria de TIC na tomada de medidas corretas para melhor proteger as crianças dos riscos de danos online, enquanto as capacita a navegar no mundo online da melhor maneira possível. A tipologia abaixo ajudará a fornecer uma compreensão mais clara de alguns dos públicos-alvo e como eles se encaixam nas listas de verificação da seção seguinte. Deve-se notar que estes são apenas alguns exemplos de categorias específicas e não são exaustivos:

- (a) Provedores de serviços de Internet, inclusive por meio de serviços de banda larga fixa ou serviços de dados celulares de operadoras de rede móvel: embora isso normalmente reflita serviços oferecidos por um período mais longo para clientes assinantes, também pode ser estendido a empresas que fornecem hotspots de WI-FI público gratuito ou pago.
- (b) Plataformas de redes sociais/mensagens e plataformas de jogos online.
- (c) Fabricantes de hardware e software, como fornecedores de dispositivos portáteis, incluindo telefones celulares, consoles de jogos, dispositivos domésticos baseados em assistência de voz, Internet das Coisas e brinquedos inteligentes conectados à Internet para crianças.
- (d) Empresas que fornecem mídia digital (criadores de conteúdo, fornecimento de acesso ou hospedagem de conteúdo).
- (e) Empresas que fornecem serviços de streaming, incluindo streams ao vivo.
- (f) Empresas que oferecem serviços de armazenamento de arquivos digitais, provedores de serviços baseados em nuvem.

5 Listas de verificação de recursos específicos

Este capítulo complementa a lista de verificação geral anterior para a indústria, oferecendo recomendações para empresas que fornecem serviços com recursos específicos sobre como respeitar e apoiar os direitos das crianças online. As seguintes listas de verificação de recursos específicos descrevem maneiras de complementar os princípios e abordagens comuns apresentados na Tabela 1, conforme se aplicam a diferentes serviços e, portanto, devem ser considerados além das etapas na Tabela 1.

Os recursos destacados aqui são transversais e várias listas de verificação de recursos específicos podem ser relevantes para a mesma empresa.

As seguintes listas de verificação de recursos são organizadas e se referem às mesmas áreas-chave que as diretrizes gerais na Tabela 1. Cada uma das listas de verificação de recursos foi desenvolvida em colaboração com os principais colaboradores e, como resultado, existem pequenas variações nas tabelas.

5.1 Recurso A: Forneça conectividade, armazenamento de dados e serviços de hospedagem

O acesso à Internet é fundamental para a realização dos direitos das crianças, e a conectividade pode abrir mundos inteiros para as crianças. Os provedores de conectividade, armazenamento de dados e serviços de hospedagem têm enormes oportunidades de criar segurança e privacidade em suas ofertas para crianças e jovens. Esta funcionalidade do serviço abrange, entre outros, operadores móveis, fornecedores de serviços de Internet, sistemas de armazenamento de dados e serviços de hospedagem.

As operadoras de celular permitem o acesso à Internet e oferecem uma variedade de serviços de dados específicos para celular. Muitas operadoras já assinaram os códigos de práticas PIO e oferecem uma variedade de ferramentas e recursos de informação que apoiam seus compromissos.

A maioria dos provedores de serviços de Internet atuam como um canal, fornecendo acesso para e da Internet, e um repositório de dados por meio de seus serviços de hospedagem, cache e armazenamento. Como resultado, eles têm a responsabilidade primária de proteger as crianças online.

Acesso à Internet em espaços públicos

Está se tornando cada vez mais comum que municípios, varejistas, empresas de transporte, cadeias de hotéis e outras empresas e organizações forneçam acesso à Internet por meio de hotspots de Wi-Fi. Esse acesso é normalmente gratuito ou fornecido a um custo mínimo e, às vezes, com formalidades mínimas de inscrição como um serviço público ou por uma empresa para atrair clientes para suas instalações ou persuadir mais pessoas a usarem seus serviços.

Promover o uso do Wi-Fi é uma forma eficaz de garantir a disponibilidade da Internet em uma determinada área. Deve-se ter cuidado, entretanto, quando esse acesso for fornecido em espaços públicos onde crianças provavelmente estarão presentes regularmente. Os usuários precisam estar cientes do fato de que os sinais de Wi-Fi podem estar disponíveis para os transeuntes e os dados do usuário podem ser comprometidos. O provedor de Wi-Fi, portanto, nem sempre será capaz de

oferecer suporte ou supervisionar o uso de uma conexão de Internet fornecida e os usuários precisam, portanto, tomar precauções para não compartilhar informações confidenciais em redes públicas de Wi-Fi.

Em espaços públicos, os provedores de Wi-Fi podem querer considerar medidas adicionais para proteger crianças e jovens, como:

- Bloqueio proativo do acesso a endereços da web conhecidos por conterem conteúdo impróprio para um grande público, além de seus esforços para bloquear o acesso ao CSAM.
- Inclusão de cláusulas nos termos e condições de uso que proíbem a utilização de serviços wi-fi para acessar ou exibir qualquer material que possa ser impróprio em um ambiente onde crianças estejam presentes. Os termos e condições também devem incluir mecanismos claros sobre as consequências de violações de tais regras.
- Tomar todas as medidas para se proteger contra o acesso não autorizado, que pode resultar na manipulação ou perda de dados pessoais.
- Instalação de filtros no sistema Wi-Fi para reforçar a política de material impróprio.
- Fornecer procedimentos e software para sinalizar e oferecer controle parental opcional relacionado ao acesso de crianças e jovens ao conteúdo da Internet.

Boa prática: Os regulamentos de telecomunicações da maioria dos estados membros da União Europeia, por exemplo, estipulam que o acesso à rede deve ser identificado, através de cartões SIM individuais ou outras ferramentas de identificação.

A Tabela 2 fornece orientação para provedores de conectividade, armazenamento de dados e serviços de hospedagem sobre as ações que podem ser realizadas para melhorar a proteção online infantil e a participação das crianças.

Tabela 2: Lista de verificação PIO para o Recurso A: Forneça conectividade, dados e dispositivos de hospedagem

Integrando considerações com os direitos da criança em todas as políticas corporativas apropriadas e processos de gestão	Provedores de conectividade, armazenamento de dados e serviços de hospedagem devem identificar, prevenir e mitigar os impactos adversos das TICs sobre processos conjuntos, e identificar oportunidades para o avanço de seus direitos. Consulte as diretrizes gerais na Tabela 1.
Desenvolvendo processos padronizados para lidar com Material pornográfico infantil (CSAM)	Em colaboração com o governo, agentes policiais, sociedade civil e organizações de linha direta, provedores de conectividade, armazenamento de dados e os serviços de hospedagem podem desempenhar um papel fundamental no combate ao material pornográfico infantil adotando as seguintes ações: Colaborar com o governo, as forças policiais, a sociedade civil e organizações de linha direta para lidar com material pornográfico infantil e relatar casos às autoridades competentes. Se uma relação entre a polícia e uma linha direta ainda não existir, envolva-se com eles para desenvolver processos conjuntos. Provedores de conectividade, armazenamento de dados ou serviços de hospedagem também podem fornecer treinamento sobre TICs para as forças policiais. Se uma empresa está operando em mercados aonde a legislação e supervisão da lei sobre este assunto é menos desenvolvida, pode encaminhar aqueles que desejam apresentar relatórios à Associação Internacional de Linhas Diretas da Internet (INHOPE) onde as denúncias podem ser feitas em qualquer linha direta internacional. Considerar a implantação de listas de bloqueio de URLs ou sites que sejam criadas por autoridades competentes (por exemplo, a polícia nacional, linhas direta, Cybertip Canada, Interpol, IWF), para dificultar o acesso dos usuários ao CSAM já identificado. Desenvolver processos de notificação, retirada e denúncia, e vincular denúncias de abuso a esses processos com um acordo de serviço público sobre o procedimento de resposta e tempo de retirada. Veja, por exemplo, o Guia do UNICEF e GSMA sobre políticas de notificação e práticas de remoção de conteúdo.

Desenvolvendo processos padronizados para lidar com Material pornográfico infantil (CSAM) (cont.)

Configurar um mecanismo de relatório com informações claras sobre seu uso para, por exemplo, dar orientação sobre o conteúdo e conduta ilegal que deve ser denunciado e esclarecer quais materiais não podem ser anexados com o relatório para evitar uma maior distribuição na web.

Apoiar a polícia em caso de investigações criminais através de atividades como a coleta de evidências.

Use os termos e condições de serviço para proibir especificamente o uso de serviços para armazenar, compartilhar ou distribuir material pornográfico infantil. Certificar que estes termos afirmam claramente que o material pornográfico infantil não será tolerado.

Certificar que os termos de serviço e condições declaram que a empresa irá cooperar totalmente com as investigações da polícia caso o material pornográfico for descoberto ou relatado.

Existem atualmente duas soluções para denunciar material pornográfico infantil online a nível nacional: linhas diretas e portais de denúncia. Uma lista completa e atualizada de todas as linhas diretas e portais existentes pode ser encontrada no INHOPE.

Linhas diretas: caso não houver uma linha direta nacional disponível, explore as oportunidades para configurar uma (consulte o Guia de linhas diretas GSMA INHOPE para uma série de opções, incluindo trabalhar com o INHOPE e a Fundação INHOPE).

Uma versão interativa do guia GSMA INHOPE está disponível, e fornece orientação sobre como desenvolver processos para a equipe de atendimento ao cliente apresentar denúncias de conteúdo questionável tanto à polícia como a INHOPE.

Portais de denúncia: O IWF oferece uma solução de portal de denúncia que permite que os usuários da Internet em países e nações sem linhas diretas, denunciem imagens e vídeos de suspeita de abuso sexual infantil diretamente à IWF por meio de uma página de portal online personalizado.

No caso de provedores de conectividade, armazenamento de dados e serviços de hospedagem cujos serviços envolvem algum tipo de hospedagem de conteúdo (muitos não envolvem), os processos de notificação e retirada de conteúdo devem estar em vigor.

Criando um ambiente digital mais seguro e apropriado à faixa etária

Provedores de conectividade, armazenamento de dados e serviços de hospedagem devem ajudar a criar um ambiente digital mais seguro e agradável para as crianças de todas as idades, realizando as seguintes ações:

Provedores de serviços de armazenamento/hospedagem de dados devem considerar apresentar a função de denúncia em todas as páginas da web e serviços, e desenvolver e documentar processos claros para gerenciar rapidamente denúncias de abuso ou outras violações dos termos e condições.

Os provedores de conectividade devem oferecer controles técnicos de marca própria ou sinalizar a disponibilidade de ferramentas criadas por fornecedores especializados que são apropriados para os serviços oferecidos e fáceis para o usuário final implementar e oferecer a possibilidade de bloquear ou filtrar acesso à Internet através das redes da empresa. Fornecer mecanismos de verificação de idade apropriados caso a empresa ofereça conteúdo ou serviços (incluindo marca própria ou serviços de terceiros que são promovidos pela empresa), que são apenas legais ou apropriados para usuários adultos (por exemplo, certos jogos, loterias).

Educando crianças, pais e educadores sobre a segurança das crianças e o seu uso responsável das TICs

Provedores de conectividade, armazenamento de dados e serviços de hospedagem devem ecoar as mensagens principais dos termos e condições da comunidade sobre as diretrizes de segurança das crianças, escritas em linguagem de fácil compreensão para apoiar as crianças, seus pais e responsáveis. Dentro do próprio serviço, no momento de upload de conteúdo, lembretes devem ser incluídos sobre tópicos como o tipo de conteúdo que é considerado inapropriado.

Fornecer às crianças e jovens informações sobre as formas mais seguras de usar a Internet. Considere maneiras criativas de promover mensagens-chave, como as seguintes:

"Nunca compartilhe quaisquer detalhes de contato, inclusive sua localização física e o seu número de telefone, com alguém que você não conhece pessoalmente."

"Nunca marque um encontro com alguém que você conheceu online sozinho(a), sem consultar um adulto primeiro. Sempre informe um amigo de confiança onde está indo ou aonde está."

"Não responda a mensagens de bullying, ou mensagens obscenas ou ofensivas. Mas guarde as evidências - não exclua a mensagem."

"Conte a um adulto ou amigo de confiança se você se sentir desconfortável ou chateado com algo ou alguém."

"Nunca compartilhe a sua senha ou nome de usuário! Esteja ciente de que outras pessoas que estão no ambiente online podem te dar informações falsas para convencê-lo a compartilhar suas informações privadas."

Os provedores de serviços podem fazer parceria com organizações que estão bem posicionadas para educar e apoiar as crianças sobre o uso mais seguro da Internet e questões relacionadas.

Consulte o Helpline International e o guia prático da GSMA para Child Helplines and Mobile Operators: Working together to protect children's rights (Linhas de Apoio e Operadores de Telefonia Móvel: Trabalhando junto para proteger os direitos das crianças) por exemplo.

Promovendo a tecnologia digital como forma de engajamento cívico

Consulte as diretrizes gerais na Tabela 1.

5.2 Recurso B: Ofereça conteúdo digital com curadoria

A Internet oferece todos os tipos de conteúdo e atividades, muitos dos quais são destinados a crianças e jovens. Os serviços que oferecem conteúdo com curadoria editorial têm enormes oportunidades de criar segurança e privacidade em seus conteúdos para crianças e jovens.

Esse recurso de serviço aborda tanto as empresas que estão criando seu próprio conteúdo quanto aquelas que estão permitindo o acesso a conteúdo digital. Refere-se, nomeadamente, a serviços de streaming de notícias e multimídia, radiodifusão de serviço público e nacional e à indústria de games.

A Tabela 3 inclui orientações para provedores de serviços que oferecem conteúdo com curadoria editorial em relação à políticas e ações que podem ser adotadas para melhorar a proteção e a participação online da criança.

Tabela 3: Lista de verificação da PIO para o recurso B: ofereça conteúdo digital com curadoria

Integrando as considerações dos direitos da criança em todas as políticas corporativas e processos de gestão	Serviços que fornecem conteúdo digital com curadoria podem ajudar a identificar, prevenir e mitigar impactos adversos das TICs nos direitos das crianças e jovens e identificar oportunidades para apoiar o avanço dos direitos das crianças e jovens ao adotar as seguintes ações: Desenvolver políticas que salvaguardem o bem-estar das crianças e jovens que contribuem com conteúdo online, que levem em conta o bem-estar físico e emocional e a dignidade de menores de 18 anos que estão envolvidos em programações, filmes, jogos, notícias, etc., independentemente do consentimento dado por um dos pais ou outro adulto.
Desenvolvendo processos padronizados para lidar com material pornográfico infantil (CSAM)	Em colaboração com o governo, agentes policiais, sociedade civil e organizações de linha direta, empresas que oferecem serviços digitais com curadoria de conteúdo podem desempenhar um papel fundamental no combate ao material pornográfico infantil através das seguintes ações: Em casos de material pornográfico infantil, por exemplo através de “comentário” ou recursos de “revisão” pelos quais os usuários têm a capacidade de fazer upload de conteúdo, a equipe deve entrar em contato com a equipe de gestão executiva responsável por denunciar tais materiais às autoridades competentes. Além disso, eles devem: • alertar as agências nacionais de aplicação da lei imediatamente; • alertar seu gerente e denunciar o material para o gestor da política de proteção de crianças; • contatar o serviço de investigação interna por telefone ou e-mail com detalhes sobre o incidente e para solicitar conselhos; • aguardar o conselho da agência relevante antes de excluir o material, salvando-o em um espaço compartilhado ou encaminhando-o.

Desenvolvendo processos padronizados para lidar com material pornográfico infantil (CSAM)

Se o material for identificado, ele deve ser denunciado diretamente para uma organização especializada em segurança na Internet que opera um sistema de denúncias de linha direta para que membros do público e profissionais de tecnologia da informação relatem formas específicas de conteúdo online potencialmente ilegal.

Por exemplo, com base em sua Política de Proteção e Salva-guarda da Criança a BBC lançou orientações editoriais sobre a interação com crianças e jovens online. Desenvolveu outras listas de verificação e códigos de conduta para trabalhar com crianças e jovens online, que também se estendem aos terceirizados e fornecedores externos. Política da Ofcom para proteção de crianças no Reino Unido aborda conteúdo online, dispositivos móveis e consoles de jogos separadamente.

Implementar uma estratégia de escalonamento rápida e robusta se o CSAM for postada ou há suspeita de conduta ilegal. Para assegurar isto:

- ofereça aos usuários um método simples e de fácil acesso para alertar o produtor de conteúdo sobre violações de quaisquer regras da comunidade online;
- remova conteúdo que viola as regras;
- ofereça aos usuários um método simples e de fácil acesso para alertar o produtor de conteúdo sobre violações de quaisquer regras da comunidade online;
- remova conteúdo que viola as regras; Antes de postar conteúdo com curadoria editorial sensível à faixa etária em um site de rede social, esteja ciente dos termos e condições do site.

Seja sensível aos requisitos de idade mínima em diferentes sites de redes sociais.

Os termos e condições de cada espaço online também devem incluir mecanismos de denúncia claros para violações de tais regras.

Criação de um ambiente online seguro e apropriado à faixa-etária

As empresas que oferecem conteúdo digital com curadoria podem ajudar a criar um ambiente digital mais seguro e agradável para crianças e jovens de todas as idades, realizando as seguintes ações:

Trabalhar com outros na indústria para desenvolver sistemas de classificação de conteúdo/ classificação etária baseados em padrões nacionais ou internacionais aceitos e consistentes com abordagens adotadas em mídias equivalentes.

Sempre que possível, as classificações de conteúdo devem ser consistentes em diferentes plataformas de mídia, por exemplo, um trailer de filme em uma sala de cinema e em um smartphone mostraria aos clientes as mesmas classificações.

Desenvolver produtos adequados para crianças e jovens, que tenham um design seguro e sejam complementados por um sistema sólido de verificação de idade.

Para ajudar os pais e outras pessoas a definir se o conteúdo é apropriado para crianças e jovens, crie aplicativos e serviços em todas as mídias que se alinhem aos sistemas de classificação de conteúdo.

Adotar métodos apropriados de verificação de idade para evitar que crianças e jovens acessem conteúdo, sites, produtos ou serviços interativos sensíveis à idade.

Fornecer conselhos e lembretes sobre a natureza e a classificação etária do conteúdo que estão usando.

Criação de um ambiente online seguro e apropriado à faixa-etária (cont.)	Uma empresa que oferece serviços audiovisuais e multimídia pode querer fornecer um número de identificação pessoal aos usuários que buscam acessar conteúdo que pode ser prejudicial para crianças e jovens.
	Garantir transparência sobre os preços dos produtos e serviços, e o uso das informações coletadas sobre usuários. Certificar que as políticas de coleta de dados estejam em conformidade com as leis aplicáveis relativas à privacidade de crianças e jovens, incluindo se o consentimento dos pais é necessário antes que empresas comerciais possam coletar informações pessoais de ou sobre uma criança.
	Certificar que a publicidade ou comunicação comercial seja claramente reconhecível como tal.
	Supervisionar o conteúdo disponibilizado online e adaptar-o aos grupos de usuários que têm probabilidade de acessá-lo, por exemplo, estabelecendo políticas adequadas para a publicidade online que atinge crianças e jovens. Se a oferta de conteúdo oferece suporte a um elemento interativo, como comentários, fóruns online, redes sociais, plataformas de jogos, salas de bate-papo ou quadros de mensagens, comunicar um conjunto claro de “regras da casa” em uma linguagem amigável ao cliente dentro dos termos de serviço e diretrizes do usuário.
	Decidir o nível de engajamento desejado antes de lançar um serviço online. Os serviços voltados para o público infantil devem apresentar apenas conteúdo adequado para o público jovem. Em caso de dúvida, as autoridades nacionais responsáveis pela proteção da criança podem ser consultadas.
	Fornecer uma rotulagem de conteúdo clara e factual. Estar ciente de que os usuários podem chegar a conteúdo impróprio seguindo links em sites de terceiros que ignoram as páginas de contextualização.
Educar crianças, pais e educadores sobre a segurança e o uso responsável das TICs.	Empresas que oferecem conteúdo digital com curadoria podem complementar medidas técnicas com atividades educacionais visando o empoderamento das crianças, tomando as seguintes ações:
	Fornecer aos clientes informações específicas e claras sobre conteúdo, como o tipo de conteúdo, classificação etária/restrições, linguagem forte ou violência e os controles parentais correspondentes disponíveis; e sobre como denunciar o uso indevido e conteúdo impróprio ou ilegal, e como as denúncias serão tratadas.
	No mundo interativo, essas informações devem ser fornecidas em forma de rótulos de conteúdo para cada programa.
	Incentivar os adultos, principalmente pais, responsáveis e educadores, a se envolverem com o consumo de conteúdo online de crianças e jovens, para que possam auxiliar e orientar crianças e jovens na escolha do conteúdo na hora da compra e para estabelecer regras de comportamento.
	Ajudar as crianças (e os pais e responsáveis) a aprender a administrar seu tempo de tela e a entender como usar a tecnologia de uma forma que seja boa para eles, incluindo o momento de parar e fazer outra coisa.
	Disponibilizar regras de uso em linguagem clara e acessível que encoraje crianças e jovens a serem vigilantes e responsáveis ao navegar a Internet.

Educar crianças, pais e educadores sobre a segurança e o uso responsável das TICs. (cont.)	Criar ferramentas adequadas à idade, como tutoriais e centros de ajuda. Trabalhar com programas de prevenção online ou presenciais e clínicas de aconselhamento quando apropriado. Por exemplo, se houver o risco de crianças e jovens se envolverem demais com a tecnologia, dificultando o desenvolvimento de relacionamentos pessoais ou a participação em atividades físicas saudáveis, um site pode fornecer um link de contato para uma linha de ajuda ou serviço de aconselhamento. Tornar as informações de segurança, como links para conselhos, proeminentes, facilmente acessíveis e claros quando o conteúdo online tiver probabilidade de atrair uma alta proporção de crianças e jovens.
	Oferecer uma ferramenta de orientação aos pais, como um “bloqueio” para controlar o conteúdo que pode ser acessado por meio de um navegador específico
	Cooperar com pais para garantir que as informações divulgadas na Internet sobre as crianças não as coloquem em risco. A forma como as crianças são identificadas em conteúdos com curadoria editorial requer uma consideração cuidadosa e varia de acordo com o contexto. Obter o consentimento informado das crianças ao apresentá-las em programas, filmes, vídeos etc., sempre que possível, e respeitar qualquer recusa em participar.
Promoção da tecnologia digital como um modo de promover o engajamento cívico	As empresas que oferecem conteúdo digital com curadoria podem incentivar e empoderar crianças e jovens, apoiando seu direito de participação por meio das seguintes ações: Desenvolver e/ou oferecer uma variedade de conteúdo de alta qualidade, desafiador, educacional, agradável e interessante que seja apropriado para a idade e auxilie crianças e jovens a dar sentido ao mundo em que vivem. Além de atraente e utilizável, confiável e seguro, esse conteúdo pode contribuir ao desenvolvimento físico, mental e social de crianças e jovens, proporcionando novas oportunidades de entretenimento e educação. Conteúdo que capacita as crianças a abraçar a diversidade e serem modelos positivos deve ser fortemente encorajado.

5.3 Recurso C: hospedar conteúdo gerado pelo usuário e conectar usuários

Foi se o tempo em que o mundo online era dominado por adultos, mas agora está claro que crianças e jovens são os principais participantes em várias plataformas na criação e compartilhamento e na explosão de conteúdo gerado pelo usuário. Este recurso de serviço aborda, entre outros, serviços de mídia social, aplicativos e sites relacionados à realização criativa.

Os serviços que conectam usuários entre si podem ser divididos em três categorias:

- Aplicativos principalmente de mensagens (Facebook Messenger, Groupme, Line, Tinder, Telegram, Viber, WhatsApp).
- Serviços principalmente de redes sociais que buscam e hospedam conteúdo gerado pelo usuário e permitem que os usuários compartilhem conteúdo e se conectem dentro e fora de suas redes (Instagram, Facebook, SnapChat, TikTok).

- Principalmente aplicativos de transmissão ao vivo (Periscope, BiGo Live, Facebook Live, Houseparty, YouTube Live, Twitch, GoLive).

Os provedores de serviços solicitam uma idade mínima para se inscrever nas plataformas, o que é difícil de aplicar, pois a verificação da idade depende da idade informada. A maioria dos serviços que conectam novos usuários entre si também permitem recursos de compartilhamento de localização, o que torna as crianças e jovens que usam esses serviços ainda mais suscetíveis aos perigos offline.

A Tabela 4, que foi adaptada de regras aplicadas por uma das maiores redes sociais, fornece orientação para provedores de serviços que hospedam conteúdo gerado pelo usuário e conectam novos usuários sobre políticas e ações que eles podem tomar para melhorar a proteção online infantil assim como a participação infantil.

Tabela 4: Lista de verificação PIO para o recurso C: hospede conteúdo gerado pelo usuário e conecte usuários

Integrando os direitos da criança em todas as políticas corporativas e processos de gestão	Serviços de hospedagem de conteúdo gerado pelo usuário e que conectam usuários podem identificar, prevenir e mitigar os impactos adversos das TICs nos direitos das crianças e jovens, e identificar oportunidades para o avanço de seus direitos.
	Consulte as diretrizes gerais na Tabela 1.
Desenvolvendo processos padronizados para lidar com Material pornográfico infantil (CSAM)	Em colaboração com o governo, agentes policiais, sociedade civil e organizações de linha direta, empresas que hospedam conteúdo criado pelos usuários e conectam usuários podem desempenhar um papel fundamental no combate ao CSAM adotando as seguintes medidas:
	Estabelecer procedimentos em todos os sites para fornecer assistência imediata à polícia durante emergências e investigações de rotina.
	Especificar que a empresa irá cooperar totalmente com as investigações policiais no caso de uma denúncia de conteúdo ilegal e detalhar penalidades como multas ou cancelamento de privilégios de faturamento.
	Trabalhar com os departamentos internos, como atendimento ao cliente, prevenção de fraude e segurança para garantir que a empresa possa reportar suspeitas de conteúdo ilegal diretamente para às autoridades e linhas diretas. Se possível, isso deve ser feito de forma a não expor a equipe da linha de frente ao conteúdo ou revitimizar a criança/crianças e jovens afetados. Para abordar situações onde a equipe pode ser exposta a material abusivo, implemente uma política ou programa para apoiar a resiliência segurança e o bem-estar da equipe.
	Use os termos e condições de serviço para proibir conteúdo e comportamento ilegais, destacando que: • conteúdo prejudicial, incluindo suspeita de aliciamento de crianças com a intenção de abuso com ou sem contato, não será tolerado; • conteúdo ilegal, incluindo o upload ou posterior disseminação de material pornográfico infantil, não será tolerado; • a empresa consultará e colaborará totalmente com as investigações policiais no caso de conteúdo ilegal, ou qualquer violação da política de proteção infantil, ser denunciado ou descoberto.

Desenvolvendo processos padronizados para lidar com Material de abuso infantil.(cont.)

Documente as práticas que a empresa tem para lidar com material pornográfico infantil, começando com o monitoramento e estendendo-se até a transferência final e destruição do conteúdo. Incluir na documentação uma lista de todo o pessoal responsável pelo manuseio do material.

Adotar políticas relativas à propriedade de conteúdo gerado pelo usuário, incluindo a opção de remover conteúdo criado pelos usuários mediante a solicitação de um usuário. Remover o conteúdo que viola as políticas do provedor e alertar o usuário que o postou sobre a violação.

Indicar que a falha de um usuário em cumprir as políticas de uso aceitável terá consequências, incluindo:

- remoção de conteúdo, suspensão ou encerramento de sua conta;
- revogação de sua capacidade de compartilhar determinados tipos de conteúdo ou usar certos recursos;
- impedimento de seu contato com crianças;
- denúncias à polícia.

Desenvolvendo processos padronizados para lidar com material de abuso sexual infantil

Promover mecanismos de denúncia para material pornográfico infantil ou qualquer outro conteúdo ilegal e garantir que os clientes saibam como denunciar se eles descobrirem esse conteúdo.

Construir sistemas e garantir que a equipe é treinada para avaliar questões de acordo com cada caso e tomar as medidas adequadas. Estabelecer equipes de operação de suporte ao usuário abrangentes e bem assessorados. Idealmente, essas equipes seriam treinadas para lidar com diferentes tipos de incidentes, a fim de garantir que uma resposta adequada é fornecida e as ações apropriadas são tomadas. Quando o usuário registra uma reclamação, dependendo do tipo de incidente, deve ser encaminhada para a equipe correta.

A empresa também pode montar equipes especiais para lidar com as denúncias do usuário em instâncias em que tais denúncias forem apresentadas com erro.

Implementar processos para remover ou bloquear imediatamente o acesso a material pornográfico infantil, incluindo processos de notificação e remoção para remover conteúdo ilegal assim que for identificado. Certificar que terceiros com os quais a empresa tem uma relação contratual tenham semelhantes e robustos processos de notificação e remoção em vigor.

Se a legislação permitir, o material pode ser guardado como prova de um crime em caso de investigações.

Desenvolver sistemas técnicos que podem detectar conteúdo ilegal conhecido e impedir que seja postado, inclusive em grupos privados ou marcá-lo para ser revisado imediatamente pela equipe de segurança da empresa. Tomar todas as medidas relevantes para proteger os serviços de serem mal utilizados para hospedar, disseminar ou criar material pornográfico infantil.

Sempre que possível, criar medidas técnicas proativas para analisar os objetos e metadados vinculados a um perfil de forma a detectar comportamentos ou padrões criminosos e tome as medidas adequadas.

Criação de um ambiente online mais seguro e adequado à faixa etária

Se o aplicativo ou serviço permite que os clientes façam upload e armazenem fotografias em servidores que pertencem ou são operados pela empresa, tenha processos e ferramentas para identificar imagens com maior probabilidade de conter material pornográfico infantil. Considere técnicas de identificação pró-ativa como tecnologia de digitalização ou revisão humana.

Os provedores de serviços que oferecem conteúdo gerado pelo usuário e conectam usuários podem ajudar a criar um ambiente digital mais seguro e agradável para crianças de todas as idades, realizando as seguintes ações:

Comunicar em uma linguagem amigável ao cliente dentro dos termos de serviço e diretrizes do usuário, um conjunto claro de "regras da casa" que definem:

- a natureza do serviço e o que se espera de seus usuários;
- o que é e o que não é aceitável em termos de conteúdo, comportamento e linguagem, além de proibir o uso ilegal;
- as consequências de qualquer violação, por exemplo, denúncia às autoridades policiais e suspensão da conta do usuário.

As principais mensagens legais e de segurança devem ser apresentadas em um formato adequado à idade (ou seja, utilizando ícones e símbolos intuitivos), em tempo hábil tanto no momento da inscrição quanto à medida que diferentes ações são realizadas no site.

Facilitar que os clientes relatem ao atendimento ao cliente suas preocupações sobre o uso indevido, estabelecendo processos padronizados e acessíveis para lidar com diferentes preocupações, como receber comunicações indesejadas (spam, bullying) ou visualizar conteúdo impróprio.

Fornecer configurações de compartilhamento e visibilidade de conteúdo adequadas à idade. Por exemplo, desenvolver configurações de privacidade e visualização que sejam mais restritivas para crianças e jovens do que as configurações padronizadas para adultos.

Aplicar requisitos de idade mínima e apoiar a pesquisa e o desenvolvimento de novos sistemas de verificação de idade, como a biometria, usando padrões internacionais conhecidos para o desenvolvimento de tais ferramentas. Tomar medidas para identificar e remover usuários menores de idade que tenham falsificado sua idade para obter acesso. Analisar a coleta adicional de dados pessoais que isso pode acarretar e a necessidade de limitar a coleta, o armazenamento e o processamento dessas informações.

Se ainda não estiver em vigor, configurar processos de login apropriados para determinar se os usuários têm idade suficiente para acessar o conteúdo ou serviço sem comprometer sua identidade, localização e detalhes pessoais. Usar sistemas funcionais de verificação de idade estabelecidos nacionalmente, conforme apropriado, onde houver medidas relevantes para assegurar privacidade de dados das crianças. Uma função de denúncia ou uma central que pode encorajar os usuários a denunciar pessoas que falsificaram suas idades.

Proteger os usuários mais jovens de comunicações indesejadas e garantir que as diretrizes de privacidade e coleta de informações estejam em vigor.

Criação de um ambiente online mais seguro e adequado à faixa etária (cont.)

Encontrar maneiras de revisar imagens e vídeos hospedados e excluir os inadequados quando detectados. Ferramentas como varredura de hash de imagens conhecidas e software de reconhecimento de imagem estão disponíveis para ajudar nisso. Em serviços direcionados a crianças, fotos e vídeos podem ser verificados com antecedência para garantir que as crianças não publiquem informações pessoais confidenciais sobre si mesmas ou outras pessoas.

Uma série de medidas podem ser usadas para controlar o acesso ao conteúdo gerado pelo usuário e proteger crianças e jovens que estão online contra conteúdo impróprio ou ilegal. Certificar que senhas seguras sejam usadas em jogos e outras configurações de mídia social como uma medida para proteger crianças e jovens. Outras técnicas incluem:

- revisar grupos de discussão para identificar assuntos prejudiciais, discurso de ódio e comportamento ilegal e excluir esse conteúdo sempre que for verificado que viola os termos de uso;
- desenvolver ferramentas para buscar e remover ativamente conteúdo que seja ilegal ou que viole os termos e condições de serviço da empresa, bem como ferramentas para impedir o envio de conteúdo ilegal conhecido para o site;
- quadros de mensagens moderados previamente com uma equipe de moderadores especializados em crianças e jovens que fazem a triagem de conteúdo que está em contradição com as "regras da casa" publicadas. Cada mensagem pode ser verificada antes de ser publicada, e os moderadores também podem identificar e sinalizar usuários suspeitos, bem como usuários em apuros;
- estabelecer uma equipe de hosts da comunidade que sirva como o primeiro ponto de contato para os moderadores quando eles tiverem preocupações sobre um usuário.

Seja responsável por revisar o conteúdo comercial, inclusive em fóruns, redes sociais e sites de jogos. Implementar normas e regras adequadas para proteger as crianças de publicidades inadequadas à idade e estabelecer limites claros para a publicidade online que atinge crianças e jovens.

Educar crianças, pais e educadores sobre a segurança das crianças e seu responsável das TICs

Os provedores de serviços que oferecem conteúdo gerado pelo usuário podem complementar medidas técnicas com medidas educacionais e atividades de capacitação, tomando as seguintes ações:

Criar uma seção dedicada a dicas de segurança, artigos, recursos e diálogo sobre cidadania digital, bem como links para conteúdo de especialistas terceirizados. Os conselhos de segurança devem ser facilmente identificados e fornecidos em uma linguagem fácil de entender. Provedores de plataformas também são encorajados a ter interfaces de navegação uniforme em diferentes dispositivos, como computadores, tablets ou telefones celulares.

Oferecer aos pais informações claras sobre os tipos de conteúdo e serviços disponíveis, incluindo, por exemplo, uma explicação sobre sites de relacionamento e serviços baseados em localização, explicar como a Internet é acessada por meio de dispositivos móveis e as opções disponíveis para aplicarem controles parentais.

Informar os pais sobre como denunciar abuso, uso indevido e conteúdo impróprio ou ilegal e como as denúncias serão tratadas. Informar quais serviços têm restrição de idade e outras maneiras de se comportar com segurança e responsabilidade ao usar serviços interativos

	Estabelecer um sistema baseado em “confiança e reputação” para encorajar bom comportamento e permitir que os colegas ensinem melhores práticas uns aos outros através de seu exemplo. Promover a importância da denúncia social, que permite que as pessoas alcancem outros usuários ou amigos de confiança para ajudar a resolver um conflito ou abrir uma conversa sobre conteúdo questionável
	Fornecer conselhos e lembretes sobre a natureza de um determinado serviço ou conteúdo e como apreciá-lo com segurança. Incluir as diretrizes da comunidade em serviços interativos, por exemplo, em pop-ups de segurança que lembrem os usuários do comportamento adequado e seguro, por exemplo, como não devem distribuir detalhes de contato.
	Cooperar com os pais e orientar-os para garantir que informações divulgadas na Internet sobre crianças não as coloquem em risco. Obter o consentimento informado das crianças quando por usar o conteúdo que elas mesmas criaram, em qualquer lugar possível, e respeite qualquer recusa.
Promover tecnologia digital como um modo de levar adiante o engajamento cívico	Serviços que hospedam conteúdo gerado pelo usuário podem encorajar e capacitar crianças e jovens, apoiando seu direito de participação.
Consulte as diretrizes gerais na Tabela 1.	

5.4 Recurso D: Sistemas movidos por inteligência artificial

Com a crescente atenção dada às tecnologias de aprendizagem profunda, os termos “inteligência artificial”, “aprendizagem de máquina” e “aprendizagem profunda” têm sido usados de forma intercambiável pelo público em geral para refletir o conceito de replicação de comportamento “inteligente” por máquinas. Nesta seção, enfocamos as maneiras como os processos de aprendizagem de máquina e aprendizagem profunda impactam a vida das crianças e, em última instância, seus direitos humanos.

“Dado o avanço exponencial das tecnologias baseadas em inteligência artificial nos últimos anos, a atual estrutura internacional que protege os direitos das crianças não aborda explicitamente muitas das questões levantadas pelo desenvolvimento e uso da inteligência artificial. No entanto, ele identifica vários direitos que podem estar implicados por essas tecnologias e, portanto, fornece um ponto de partida importante para qualquer análise de como os direitos das crianças podem ser positiva ou negativamente afetados por novas tecnologias, como os direitos à privacidade, à educação, à brincar, e à não discriminação¹⁸.”

A aplicação da IA pode afetar o impacto que diferentes serviços tem nas crianças quando são usados em redes sociais, como plataformas de streaming de vídeo. Os algoritmos de aprendizado de máquina, o mecanismo de recomendação empregado principalmente por plataformas populares de compartilhamento de vídeo, são otimizados para garantir o máximo de visualizações de vídeos específicos durante um determinado período¹⁹. A tecnologia de tela sensível ao toque (touchscreen) e o design dessas plataformas permitem que crianças muito pequenas passem por e naveguem este conteúdo. Há uma preocupação específica de que algoritmos que usam vídeos recomendados podem prender as crianças em “bolhas de filtro” de conteúdo pobre ou impróprio. Como as crianças são particularmente suscetíveis a recomendações de conteúdo, “vídeos relacionados” chocantes podem chamar sua atenção e desviá-las de uma programação mais adequada à sua idade.²⁰

A IA também impacta a proteção infantil online no que diz respeito a brinquedos inteligentes. Os distintos processos envolvidos na operação de brinquedos inteligentes vêm com seus próprios desafios, ou seja, o brinquedo (que faz interface com a criança), o aplicativo móvel, que atua como ponto de acesso para conexão Wi-Fi, e a conta online personalizada do brinquedo/consumidor, onde os dados são armazenados. Esses brinquedos se comunicam com servidores baseados em nuvem que armazenam e processam dados fornecidos pelas crianças que interagem com o brinquedo. Este modelo apresenta questões de privacidade se a segurança não for aplicada em todas as camadas, o que foi demonstrado pelos muitos casos com hackers que vazaram detalhes pessoais. Além disso, alguns dos dispositivos hackeados (incluindo dispositivos inteligentes habilitados para web, como babás eletrônicas, assistentes de voz, etc.) podem ser usados para vigiar usuários sem seu conhecimento ou consentimento.

Ao integrar mecanismos de resposta a ameaças detectadas contra crianças que usam esses dispositivos, por exemplo, fornecendo dicas e recomendações com base no comportamento detectado (como mencionado anteriormente com o aplicativo BBC Own It), é crucial que as empresas que desenvolvem os dispositivos inteligentes baseiem essas recomendações em evidências e os desenvolvam em consulta com especialistas em proteção infantil.

¹⁸ Criação de um ambiente online mais seguro e adequado à faixa etária

¹⁹ Ibid.

²⁰ Ibid.

Embora algumas empresas estejam promovendo princípios para o uso ético da IA²¹, não está claro se existem políticas públicas voltadas para IA e crianças²². Várias associações comerciais e de tecnologia e grupos de ciência da computação elaboraram princípios éticos sobre IA²³. No entanto, isso não se refere explicitamente aos direitos da criança, às formas pelas quais essas tecnologias de IA podem criar riscos para as crianças ou a planos proativos para mitigá-los.

"Assim como as corporações, os governos em todo o mundo adotaram estratégias para se tornarem líderes no desenvolvimento e uso da IA, promovendo ambientes adequados para inovadores e corporações."²⁴ Não está claro, entretanto, como essas estratégias nacionais abordam diretamente os direitos da criança.

Melhorando a maneira como o Facebook lida com o suicídio e conteúdo relacionado a automutilação

Em 2019, o Facebook começou a hospedar [consultas](#) regulares com especialistas de todo o mundo para discutir alguns dos tópicos mais difíceis associados ao suicídio e automutilação. Isso inclui como lidar com bilhetes de suicídio, os riscos relacionados a conteúdo deprimente online e representações de suicídio de interesse jornalístico. Mais detalhes dessas reuniões estão disponíveis na nova [página de Prevenção ao Suicídio](#) do Facebook, em sua [Central de Segurança](#). Essas consultas resultaram em várias melhorias na forma como o Facebook lida com esse tipo de conteúdo. A política sobre [automutilação](#), por exemplo, foi reforçada para proibir imagens gráficas de pessoas se cortando para evitar a promoção ou o desencadeamento involuntário de automutilação. Mesmo quando alguém está buscando apoio ou se expressando para ajudar em sua recuperação, o Facebook agora exibe uma tela de aviso de sensibilidade sobre imagens de cortes de automutilação. Esse tipo de conteúdo agora está sendo descoberto por meio da aplicação de IA, em que ações sobre conteúdo potencialmente perigoso, incluindo sua remoção ou a inclusão de telas de aviso de sensibilidade, podem ser executadas automaticamente. De abril a junho de 2019, o Facebook agiu em mais de 1,5 milhão de posts de suicídio e autolesão em seu site e identificou mais de 95% antes de ser relatado por um usuário. Durante o mesmo período, o Instagram atuou em mais de 800 mil peças de conteúdo semelhante, das quais mais de 77 por cento foram detectadas antes de serem relatadas por um usuário.

21 Consulte Microsoft, "Salient Human Rights Issues", Report - FY17; and Google, "Responsible Development of AI" (2018).

22 Microsoft Official Blog, "The Future Computed: Artificial Intelligence and its role in society", 2018.

23 The Guardian, "'Partnership on AI' formed by Google, Facebook, Amazon, IBM and Microsoft", 2016.

24 Ibid.

Identificar potencial bullying ou violência entre pares em tempo real e notificar usuários

O Instagram está implementando IA para erradicar comportamentos como insultos, humilhação e desrespeito. Ao usar ferramentas de denúncia sofisticadas, os moderadores podem fechar rapidamente a conta do perpetrador de bullying online.

Boas práticas: uso de inteligência artificial na identificação de material de abuso sexual infantil

Com base na generosa contribuição do PhotoDNA da Microsoft para combater a exploração infantil e o recente lançamento da API de segurança de conteúdo do Google, o Facebook também desenvolveu tecnologias para detectar conteúdo de abuso sexual infantil.

Conhecidas como PDQ e TMK + PDQF, essas tecnologias fazem parte de um conjunto de ferramentas que o Facebook usa para detectar conteúdo prejudicial. Outros algoritmos e ferramentas disponíveis para a indústria incluem pHash, aHash e dHash. O algoritmo de correspondência de fotos do Facebook, PDQ, deve muita de sua inspiração ao pHash, embora tenha sido construído do zero como um algoritmo distinto com implementação de software independente. A tecnologia de correspondência de vídeo, TMK + PDQF, foi desenvolvida em conjunto pela [equipe de Pesquisa em IA do Facebook](#) e acadêmicos da Universidade de Modena e Reggio Emilia na Itália.

Essas tecnologias criam uma maneira eficiente de armazenar arquivos como hashes digitais curtos que podem determinar se dois arquivos são iguais ou semelhantes, mesmo sem a imagem ou vídeo original. Hashes também podem ser compartilhados mais facilmente com outras empresas e organizações sem fins lucrativos.

PDQ e TMK + PDQF foram projetados para operar em alta escala, suportando hashing de quadros de vídeo e aplicações em tempo real.

Algumas das recomendações para as empresas alinharem seus princípios ao projetar e implementar soluções baseadas em IA voltadas para crianças são fornecidas na Tabela 5.

As recomendações são baseadas no trabalho do UNICEF para desenvolver diretrizes de políticas globais sobre IA e crianças, que serão destinadas a governos e indústrias. Por favor, veja <https://www.unicef.org/globalinsight/feature-projects/ai-children> para mais informações sobre o projeto. As recomendações também se baseiam no artigo do UNICEF e da UC Berkeley sobre IA e os direitos da criança²⁵.

25 UNICEF and UC Berkeley, "Executive Summary: Artificial Intelligence and Children's Rights", 2018.

Tabela 5: Lista de verificação PIO para o Recurso D: sistemas acionados por IA

Integrando considerações com os direitos da criança em todas as políticas corporativas apropriadas e processos de gestão	Os fornecedores de sistemas baseados em IA podem identificar, prevenir e mitigar os impactos adversos das TICs nos direitos das crianças e jovens, e identificar oportunidades para apoiar o avanço das crianças e os direitos dos jovens.
	Os sistemas de IA devem ser projetados, desenvolvidos, implementados e pesquisados para respeitar, promover e cumprir os direitos da criança, conforme consagrados na Convenção de Direitos da Criança. A infância, que é cada vez mais experimentada no ambiente digital, é um momento dedicado a cuidados e assistência especiais. Os sistemas de IA devem ser avançados para fornecer esse suporte em todo o seu potencial.
	Incorpore uma abordagem de design inclusivo ao desenvolver produtos voltados às crianças, que maximiza a diversidade de gênero, geográfica e cultural e inclua uma ampla gama de partes interessadas, como pais, professores, psicólogos infantis e, quando apropriado, as próprias crianças.
	Estruturas de governança, incluindo diretrizes éticas, leis, normas e órgãos reguladores, devem ser estabelecidos para supervisionar processos que garantem que a aplicação de sistemas de IA não infrinja os direitos da criança.
Desenvolvendo processos padronizados para lidar com Material pornográfico infantil (CSAM)	Em colaboração com o governo, agentes policiais, sociedade civil e organizações de linha direta, fornecedores de sistemas baseados em IA desempenham um papel fundamental no combate ao material pornográfico infantil, tomando as seguintes ações: Consulte as diretrizes gerais na Tabela 1.
Criando um ambiente digital mais seguro e apropriado à faixa etária	Os fornecedores de sistemas baseados em IA podem ajudar a criar um ambiente digital mais seguro e agradável para crianças de todas as idades, tomando as seguintes ações:
	Adotar uma abordagem multidisciplinar ao desenvolver tecnologias que afetam as crianças e consultar a sociedade civil, incluindo academia, para identificar os impactos potenciais dessas tecnologias sobre os direitos de uma ampla gama de usuários finais potenciais.
	Implementar a segurança e a privacidade desde o projeto para produtos e serviços dirigidos à ou comumente usados por crianças.
	Como os sistemas de IA são ávidos por dados, empresas que usam IA para seus serviços devem ser especialmente vigilantes em relação à coleta, processamento, armazenamento, venda e publicação de dados pessoais de crianças.
	Os sistemas de IA devem ser transparentes, no sentido de que deve ser possível descobrir como e por que um sistema tomou uma decisão particular ou, no caso de um robô, porque agiu da maneira que agiu. Essa transparência é crucial para desenvolver confiança e facilitar auditorias, investigações e entradas com recurso quando houver suspeita de danos às crianças.
	Certificar que existem mecanismos funcionais e legais de recurso se crianças forem, ou afirmam ser, prejudicadas por sistemas de IA. Devem ser estabelecidos processos para a reparação oportuna de qualquer casos discriminatórios e órgãos de supervisão criados para apelos e monitoramento contínuo da segurança e proteção das crianças. Responsabilidade e os mecanismos de reparação andam de mãos dadas.

Criando um ambiente digital mais seguro e apropriado à faixa etária (cont.)	Desenvolver planos para lidar com dados especialmente sensíveis, incluindo revelações de abuso ou outros danos que possam ser de responsabilidade compartilhada com a empresa devido à seus produtos. Plataformas digitais e sistemas de IA devem minimizar a coleta de dados sobre crianças e maximizar o controle das crianças sobre os dados que elas criam. Termos de uso devem ser compreensíveis para crianças de forma que capacite sua ciência e Empoderamento.
Educar crianças, pais e educadores sobre a segurança das crianças e seu uso responsável das TICs	Fornecedores de sistemas baseados em IA podem complementar medidas técnicas com atividades educacionais e de capacitação. O propósito dos sistemas de IA deve ser passível de ser explicado para crianças E elas devem ter o poder de recusar tais plataformas.
Promova tecnologia digital como ferramenta para aumentar o engajamento cívico	Os fornecedores de sistemas baseados em IA podem encorajar e capacitar crianças e jovens, apoiando seu direito de participação Consulte as diretrizes gerais na Tabela 1.
Usando avanços tecnológicos para proteger e educar crianças	Sistemas baseados em IA devem ser desenvolvidos para apoiar o desenvolvimento e bem-estar das crianças como resultado de todo o design desenvolvimento e implementação do sistema. A disponibilidade e aceitação das métricas de bem estar e desenvolvimento devem ser seus pontos de referência. As empresas devem investir em pesquisa e desenvolvimento de ferramentas éticas baseadas em IA para detectar atos de abuso e exploração infantil online e bullying, assédio e intimidação, em colaboração com os principais especialistas em direitos das crianças e as próprias crianças. Os avanços na tecnologia de IA devem ser aplicados à mensagens direcionadas para crianças sem comprometer sua identidade, localização e dados pessoais.

Referências

Texto do GDPR (Regulamento da UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, sobre a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e sobre a livre circulação desses dados, e revogando a diretiva 95/46/EC (Regulamento geral de proteção de dados) e texto conforme publicado no [Jornal Oficial da UE](#).

AVMS (Audio Visual Media Services) [revisto](#) que altera a Diretiva 2010/13/UE relativa à coordenação de certas disposições estabelecidas por lei, regulamento ou ação administrativa nos Estados-Membros em matéria de prestação de serviços de comunicação audiovisuais (Diretiva Serviços de Comunicação Social Audiovisual) com vista às mudanças na realidades do mercado e [Texto conforme publicado no Jornal Oficial da UE](#).

Política da BBC:

- [Política de proteção infantil, versão 2017](#), revisada 2018 e [versão atualizada 2019](#)
- [Trabalhar com jovens e crianças na BBC](#);
- Estrutura para empresas de produção independentes que trabalham na BBC Productions [sobre regras de proteção infantil para fornecedores terceirizados](#);
- Orientação: Interagindo com crianças e jovens online [sobre as diretrizes editoriais para atividades online](#).

Investigação comprovando o não respeito à verificação de idade nas redes sociais no Reino Unido: [2016](#), [2017](#); [2020](#).

Glossário

As definições abaixo foram extraídas principalmente da terminologia existente estabelecida na Convenção sobre os Direitos da Criança, 1989, bem como pelo Grupo de Trabalho Interinstitucional sobre Exploração Sexual de Crianças nas [Diretrizes de Terminologia para a Proteção de Crianças contra Exploração Sexual e Sexual Abuso](#), 2016 (Diretrizes de Luxemburgo), pela [Convenção do Conselho da Europa sobre a Proteção de Crianças contra Exploração Sexual e Abuso Sexual](#), 2007, bem como pelo [relatório do UNICEF Global Kids Online](#), 2019.

Adolescentes

Adolescentes são pessoas com idades entre 10 e 19 anos. É importante observar que o termo “adolescentes” não é vinculativo sob o direito internacional, e pessoas com menos de 18 anos são consideradas crianças, enquanto as pessoas de 18 a 19 anos são consideradas adultas, a menos que a maioridade seja atingida mais cedo de acordo com a legislação nacional.²⁶

Inteligência artificial

No sentido mais amplo, inteligência artificial (IA) se refere indistintamente a sistemas que são pura ficção científica (os chamados IAs “fortes” com uma forma de autoconsciência) e sistemas que já estão operacionais e capazes de realizar tarefas muito complexas (sistemas descritos como IAs “fracos” ou “moderados”, como reconhecimento facial ou de voz e direção de veículos).²⁷

Sistemas de inteligência artificial

Um sistema de IA é um sistema baseado em máquina que pode, para um determinado conjunto de objetivos definidos por humanos, fazer previsões, recomendações ou decisões que influenciam ambientes reais ou virtuais. Os sistemas de IA são projetados para operar em vários níveis de autonomia.²⁸

Alexa:

Amazon Alexa, conhecida simplesmente como Alexa, é uma assistente de IA virtual desenvolvida pela Amazon. É capaz de interação de voz, reprodução de música, listas de tarefas, configuração de alarmes, streaming de podcasts, reprodução de audiolivros e de fornecer dados sobre o clima, trânsito, esportes e outras informações em tempo real, como notícias. Alexa também pode controlar vários dispositivos inteligentes usando a si mesma como um sistema de automação residencial. Os usuários podem estender os recursos da Alexa instalando “habilidades” (funcionalidade adicional desenvolvida por fornecedores terceirizados, em outras configurações mais comumente chamadas de aplicativos, como programas meteorológicos e recursos de áudio).²⁹

26 UNICEF e UIT, “Guidelines for Industry on Child Online Protection”, 2014.

27 Council of Europe, “What’s AI?”.

28 OECD, “Recommendation of the Council on Artificial Intelligence”, 2019.

29 UNICEF e UIT, “Guidelines for Industry on Child Online Protection”, 2014.

Melhor interesse da criança

Refere-se a todos os elementos necessários para tomar uma decisão em uma situação específica sobre uma criança específica ou grupo de crianças.³⁰

Criança

De acordo com o artigo 1 da Convenção sobre os Direitos da Criança, criança é qualquer pessoa com menos de 18 anos, a menos que a maioridade seja atingida mais cedo de acordo com a legislação nacional.³¹

Exploração e abuso sexual infantil

Descreve todas as formas de exploração sexual e abuso sexual, por exemplo, "(a) o incentivo ou coação de uma criança para que se envolva em qualquer atividade sexual ilegal; (b) o uso exploratório de crianças na prostituição ou outras práticas sexuais ilegais; (c) o uso exploratório de crianças em apresentações e materiais pornográficos",³² bem como um "contato sexual que geralmente envolve forçar uma pessoa sem consentimento".³³ A exploração e o abuso sexual infantil ocorrem cada vez mais por meio da Internet ou de alguma forma conectados ao ambiente online.

Exploração e abuso sexual infantil

A rápida evolução das TICs criou novas formas de CSEA on-line, que podem ocorrer virtualmente e não precisam incluir um encontro em pessoa com a criança³⁴. Embora muitas jurisdições ainda rotulem as imagens e vídeos de abuso sexual infantil como "pornografia infantil" ou "imagens indecentes de crianças", estas Diretrizes referem-se às questões coletivamente como "material de abuso sexual infantil" (CSAM). Este termo está em acordo com as Diretrizes da Comissão de Banda Larga e o Modelo de Resposta Nacional da WePROTECT GlobalAlliances³⁵ e descreve o conteúdo com mais precisão. A pornografia se refere a um setor comercializado legítimo e, como afirmam as Diretrizes de Luxemburgo, o uso do termo:

"Pode (inadvertidamente ou não) contribuir para diminuir a gravidade, banalizar, ou mesmo legitimar o que é na verdade abuso sexual e/ou exploração sexual de crianças. O termo 'pornografia infantil' corre o risco de insinuar que os atos são realizados com o consentimento da criança e representam material sexual legítimo." Quando usamos o termo material pornográfico infantil, nos referimos a materiais que representam atos que são sexualmente abusivos e/ou exploradores para uma criança. Isso inclui, mas não se limita a, material que registre o abuso sexual de crianças por adultos, imagens de crianças incluídas em conduta

30 Consulte a Convenção das Nações Unidas sobre o Direito da Criança.

31 UNICEF e UIT, "Guidelines for Industry on Child Online Protection", 2014.

32 Artigo 34 da Convenção das Nações Unidas sobre o Direito da Criança.

33 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Luxembourg Guidelines), 2016.

34 The Luxembourg Guidelines (ibid), 2016 e a UNICEF Global Kids Online report, 2019.

35 Broadband Commission for Sustainable Development, "Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online", 2019; WePROTECT Global Alliance, "Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response", 2016.

sexualmente explícita e órgãos sexuais de crianças quando as imagens são produzidas ou usadas para fins principalmente sexuais.

Consulte as [Diretrizes de Luxemburgo](#) para termos como “material de abuso sexual infantil gerado digitalmente e no computador”.

Crianças e jovens

Descreve todas as pessoas com menos de 18 anos, em que “crianças” (também referidas como “crianças mais novas” nestas diretrizes da UIT) abrange todas as pessoas com menos de 15 anos e “jovens” compreende pessoas na idade de 15-18.

Brinquedos conectados

Os brinquedos conectados se conectam à Internet usando tecnologias como Wi-Fi e Bluetooth e normalmente operam em conjunto com aplicativos complementares para permitir brincadeiras interativas para as crianças. De acordo com a Juniper Research, em 2015 o mercado de brinquedos conectados atingiu US \$ 2,8 bilhões e está previsto que aumente para US \$ 11 bilhões até 2020. Esses brinquedos coletam e armazenam informações pessoais de crianças, incluindo nomes, geolocalização, endereços, fotografias, gravações de áudio e vídeo.³⁶

Cyberbullying

O cyberbullying descreve um ato intencionalmente agressivo realizado repetidamente por um grupo ou um indivíduo usando tecnologia digital e visando uma vítima que não pode se defender facilmente³⁷. Geralmente envolve “usar a tecnologia digital e a Internet para postar informações prejudiciais sobre alguém, compartilhar propositalmente informações privadas, fotos ou vídeos de forma prejudicial, enviar mensagens ameaçadoras ou ofensivas (via e-mail, mensagem instantânea, chat ou textos), espalhar boatos e informações falsas sobre a vítima ou excluí-la propositalmente das comunicações online”.³⁸

Cyberhate (ódio cibernético), discriminação e extremismo violento

“O ódio cibernético, a discriminação e o extremismo violento são uma forma distinta de violência cibernética, pois visam uma identidade coletiva, em vez de indivíduos,... muitas vezes devido a raça, orientação sexual, religião, nacionalidade ou status de imigração, sexo/gênero e opção política”³⁹.

Cidadania Digital

Cidadania digital refere-se à capacidade de se engajar de forma positiva, crítica e competente no ambiente digital, valendo-se de habilidades de comunicação e criação eficazes, para praticar formas de participação social que respeitem os direitos humanos e a dignidade por meio do uso responsável da tecnologia⁴⁰.

36 Jeremy Greenberg, “Dangerous Games: Connected Toys, COPPA, and Bad Security”, Georgetown Law Technology Review, 2017.

37 Anna Costanza Baldry et al. “Cyberbullying and Cybervictimization versus Parental Supervision, Monitoring and Control of Adolescents’ Online Activities”, Children and Youth Services Review, 2019.

38 The Luxembourg Guidelines, 2016 and the UNICEF Global Kids Online report, 2019 (ibid).

39 UNICEF Global Kids Online report, 2019 (ibid).

40 Council of Europe, “Digital Citizenship and Digital Citizenship Education”.

Alfabetização Digital

Alfabetização digital significa ter as habilidades que uma pessoa precisa para viver, aprender e trabalhar em uma sociedade onde a comunicação e o acesso à informação acontecem cada vez por meio de tecnologias digitais, como plataformas de Internet, mídias sociais e dispositivos móveis⁴¹. Inclui comunicação clara, habilidades técnicas e pensamento crítico.

Resiliência digital

Este termo descreve a capacidade de uma criança lidar emocionalmente com os danos encontrados online. Também se refere à inteligência emocional necessária para entender quando uma criança está correndo algum risco online, saber como buscar ajuda, aprender com a experiência e se recuperar quando as coisas dão errado⁴².

Governadores

Descreve todas as pessoas que ocupam uma posição em uma estrutura de gestão ou governança escolar

Grooming/aliciamento online

Grooming/aliciamento online, conforme definido nas Diretrizes de Luxemburgo, refere-se a "o processo de estabelecer/construir um relacionamento com uma criança pessoalmente ou através do uso da Internet ou de outras tecnologias digitais para facilitar o contato sexual *online* ou *offline* com essa pessoa." É a atividade criminosa de fazer amizade com uma criança..., a fim de tentar persuadir a criança a ter uma relação sexual.

Tecnologias da Informação e Comunicação

As tecnologias de informação e comunicação (TICs) descrevem todas as tecnologias de informação que enfatizam o aspecto da comunicação. Isso inclui todos os serviços e dispositivos de conexão à Internet, como computadores, laptops, tablets, smartphones, consoles de jogos e smartwatches⁴³. Inclui também serviços como rádio e televisão, bem como banda larga, hardware de rede e sistemas de satélite.

Jogos online

Jogo online é definido como jogar qualquer tipo de jogo digital comercial envolvendo um ou vários jogadores por meio de qualquer dispositivo conectado à Internet, incluindo consoles dedicados, computadores desktop, laptops, tablets e telefones celulares. O "ecossistema de jogos online" inclui assistir outros jogarem videogames por meio de e-sports, streaming ou plataformas de compartilhamento de vídeo, que normalmente fornecem opções para os espectadores comentarem ou interagirem com os jogadores e outros membros do público⁴⁴.

41 Western Sydney University, "What is digital literacy?".

42 Dr. Andrew K. Przybylski, et al., "A Shared Responsibility: Building children's' online resilience", Virgin Media and Parent Zone, 2014.

43 UNICEF e UIT, "Guidelines for Industry on Child Online Protection", 2014 (as above).

44 UNICEF, "Child Rights and Online Gaming: Opportunities & Challenges for Children and the Industry", 2019.

Ferramentas de controle parental

Software que permite aos usuários, normalmente os pais, controlar algumas ou todas as funções de um computador ou outro dispositivo que pode se conectar à Internet. Normalmente, esses programas podem limitar o acesso a determinados tipos ou classes de sites ou serviços online. Alguns também fornecem espaço para gerenciamento de tempo, ou seja, o dispositivo pode ser configurado para ter acesso à Internet apenas em determinados horários. Versões mais avançadas podem gravar todos os textos enviados ou recebidos de um dispositivo. Os programas normalmente serão protegidos por senha⁴⁵.

Informações pessoais

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

Privacidade

A privacidade é frequentemente medida em termos de compartilhamento de informações pessoais online, ter um perfil público de mídia social, compartilhamento de informações com pessoas conhecidas online, uso de configurações de privacidade, compartilhamento de senhas com amigos e preocupações com privacidade⁴⁶.

Mídia de serviço público

Essas são emissoras ou meios de comunicação nacionais que receberam sua licença de transmissão com base em uma série de obrigações contratuais cumpridas com o estado ou parlamento. Essas obrigações foram estendidas em muitos países nos últimos anos para enfrentar as consequências da transformação digital por meio de programas de alfabetização digital e mídia e a responsabilidade de lidar com a exclusão digital.

Sexting

Sexting é comumente definido como o envio, recebimento ou troca de conteúdo sexualizado de produção própria, incluindo imagens, mensagens ou vídeos por meio de telefones celulares e/ou da Internet⁴⁷. A criação, distribuição e posse de imagens sexuais de crianças é ilegal na maioria dos países. Se imagens sexuais de crianças autoproduzidas forem reveladas, os adultos não devem vê-las. O compartilhamento de imagens sexuais por um adulto com uma criança é sempre um ato criminoso, que pode ser prejudicial e pode ser necessário denunciar essas imagens e removê-las.

45 UNICEF e UIT, "Guidelines for Industry on Child Online Protection", 2014 (ibid).

46 US Federal Trade Commission, "Children's Online Privacy Protection Act", 1998.

47 The Luxembourg Guidelines, 2016 (as above).

Sextorção ou extorsão sexual de crianças

Sextorção é a “chantagem de uma pessoa com a ajuda de imagens autogeradas dessa pessoa, a fim de extorquir favores sexuais, dinheiro ou outros benefícios dela ou dele sob a ameaça de compartilhar o material além do consentimento da pessoa retratada (por exemplo, postar imagens nas redes sociais)”⁴⁸.

Internet das Coisas

“A Internet das Coisas (IoT) representa o próximo passo para a digitalização de nossa sociedade e economia, onde objetos e pessoas são interconectados por meio de redes de comunicação e relatam sobre seu estado e/ou o ambiente ao redor.”⁴⁹

URL

Esta abreviatura significa “localizador uniforme de recursos”, o endereço de uma página da Internet⁵⁰.

Realidade virtual

“A realidade virtual é o uso da tecnologia do computador para criar o efeito de um mundo tridimensional interativo no qual os objetos têm uma sensação de presença espacial.”⁵¹

Wi-Fi

Wi-Fi (Wireless Fidelity) é o grupo de padrões técnicos que permite a transmissão de dados em redes sem fio⁵².

48 The Luxembourg Guidelines, 2016 (as above).

49 European Commission, “Policy: The Internet of Things”.

50 UNICEF and ITU, “Guidelines for Industry on Child Online Protection”, 2014 (as above).

51 NASA, “Virtual Reality: Definition and Requirements”.

52 US Federal Trade Commission, “Children’s Online Privacy Protection Act”, 1998.

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

ISBN: 978-92-61-30411-9



9 789261 304119

Publicado na Suíça
Genebra, 2020
Créditos das fotos: Shutterstock