# Privacidade *e* Proteção:

## Uma abordagem dos direitos da criança à criptografia


Autoria

CRIN CHILD RIGHTS INTERNATIONAL NETWORK

defend|digital|me

Tradução

IP rec

## Agradecimentos

Nós gostaríamos de agradecer aos entrevistados e aos respondentes dos questionários que participaram da pesquisa para este relatório e também a todos que revisaram e forneceram comentários às versões rascunho.

© Child Rights International Network e defenddigitalme 2023.

CRIN é uma think tank criativa que produz perspectivas novas e dinâmicas sobre problemas de direitos humanos, com foco no direito de crianças. Nós pressionamos por direitos - não caridade - e fazemos campanhas por uma mudança genuína em como governos e sociedades veem e tratam crianças.

A Child Rights International Network (CRIN) é registrado no Reino Unido e regulado pela Companies House and the Charity Commission (Company Limited by Guarantee No. 6653398 and Charity No. 1125925)

defenddigitalme group (defendidigtalme) é registrado no Reino Unido na Companies House (Company Limited by Guarantee No. 11831192)

Ilustrações por Miriam Sugranyes

Tradução por Pedro Amaral, Marcos Cesar M. Pereira, Raquel Saraiva, Mariana Canto, Pedro Lourenço e Luana Batista - Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec)

Revisão por Marina Meira
Diagramação por Guilherme Saraiva

Este relatório é para propósitos informacionais e educativos apenas e não deve ser utilizado como orientação legal. CRIN e defenddigitalme não tomam responsabilidade por qualquer perda, dano, custo ou gastos incorridos, ou decorrentes de qualquer pessoa utilizando ou se baseando em informações deste relatório. CRIN e defenddigitalme encorajam o uso pessoal e educacional desta publicação e permitem sua reprodução nessa capacidade na qual créditos sejam dados de boa-fé.

Este conteúdo é licenciado em Creative Commons AtributionNonCommercialNoDerivatives 4.0 licença internacional. Nenhum material produzido pelo CRIN pode ser modificado exceto se consentimento seja dado por escrito. Nenhum material produzido pelo CRIN pode ser reutilizado para ganhos comerciais, exceto se o consentimento seja dado por escrito.

Primeira publicação em janeiro de 2023.

Versão em português em novembro de 2023.

Como citar: Privacidade e Proteção: Uma abordagem do direito das crianças à criptografia. (2023) Child Rights International Network and defenddigitalme.

Tradução: Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec).



# Conteúdos

# Prefácio à versão brasileira

A versão traduzida para o idioma português do relatório "Privacy and Protection: A children's rights approach to encryption" visa trazer insumos ao debate sobre as relações entre a criptografia e os direitos de crianças e adolescentes. Esta tradução foi realizada pela equipe do Observatório da Criptografia (ObCrypto). Desde 2021, o Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec) desenvolve o Observatório da Criptografia, dedicado a monitorar políticas públicas e privadas que podem impactar o uso da criptografia forte no Brasil e no mundo.

Nós compreendemos que o debate em torno de criptografia e direito de crianças e adolescentes se encontra tensionado, sobretudo no Norte Global. Conforme discutido neste trabalho desenvolvido por Child Rights International Network (CRIN) e defenddigitalme, assim como exposto em diversas análises do ObCrypto ao longo do seu desenvolvimento e por várias organizações e especialistas, a defesa desse grupo contra ameaças online e o combate à proliferação de material de abuso sexual infantil (CSAM, no inglês Child Sexual Abuse Material) são utilizados como justificativas para o enfraquecimento de criptografia.

O ObCrypto tem se dedicado ao tema desde seu início com o texto "Criptografia é segurança para crianças e adolescentes: não está claro?", trazendo os termos desse debate. Ao longo de 2022 e 2023, nos debruçamos sobre projetos de lei que defendem algum nível de enfraquecimento da criptografia em nome da segurança de crianças e adolescentes, como o EARN IT Act (Estados Unidos), o ChatControl (União Europeia) e a recém-aprovada Online Safety Bill (Reino Unido). A legítima preocupação com a segurança de crianças e adolescentes é compartilhada também por atores da indústria. A Apple, por exemplo, chegou a apresentar uma proposta  de varredura pelo lado do cliente em seus dispositivos para identificar CSAM - prática que enfraquece a privacidade das comunicações e a segurança dos dispositivos, conforme analisado também pelo ObCrypto.

Enquanto este debate está em estágio avançado no Norte Global, no Brasil ele ainda é incipiente. Isso cria, na nossa avaliação, um risco para a utilização da criptografia e, consequentemente, para a privacidade e segurança de pessoas e organizações que fazem uso de ferramentas com criptografia forte. Opor criptografia à segurança das crianças e dos adolescentes é um argumento simplista, que tende ao aumento da vigilância e da insegurança de todas as pessoas, inclusive dessa parcela mais jovem da população.

Conjunturalmente, identificamos que as narrativas que mobilizam a defesa de crianças em plataformas criptografadas visam o combate à desinformação e o extremismo violento, como nos ataques em escolas ao redor do Brasil, que ocasionaram mortos e feridos. Com isso em mente, em 2023, produzimos a análise "Discutir criptografia e a proteção de crianças e adolescentes é urgente", analisando algumas das possibilidades pelas quais tal oposição entre a segurança e a privacidade poderia ganhar força e protagonizar o debate sobre direitos das crianças e adolescentes no meio digital no Brasil.

O relatório escrito por CRIN e defendidgitalme oferece uma abordagem valiosa para o debate, pois parte de uma perspectiva protetiva e garantista dos direitos das crianças e dos adolescentes. Um dos méritos deste relatório é trazer argumentos e perspectivas diversas para pensar a criptografia a partir dos direitos infantojuvenis. Além disso, busca trazer concretude aos problemas abordados em oposição aos recorrentes discursos que apelam para o medo, sem lançar mão de elementos empíricos.

Enquanto um texto tão rico em detalhe, um processo de tradução que preserve a qualidade do original, sem afetar a capacidade de ser compreendido pelo público brasileiro, é um desafio, dadas as diferenças entre as línguas e culturas. Por isso, queremos informar já no prefácio à versão brasileira uma das particularidades desta tradução.

No Brasil, de acordo com o Estatuto da Criança e do Adolescente (ECA), fazemos a diferenciação entre sujeitos até os doze anos incompletos (crianças) e sujeitos entre doze e dezoito anos incompletos (adolescentes). No relatório em versão original, porém, o termo "criança" é utilizado de acordo com a Convenção sobre os Direitos da Criança (CDC) da Organização das Nações Unidas para abarcar todos os indivíduos até dezoito anos incompletos. Optamos por manter o termo "criança" do original, o que significa que, ao longo deste texto traduzido, ele faz referência ao que na lógica do ECA são crianças e adolescentes.

Vale também notar que buscamos traduzir termos técnicos, inclusive nas notas de rodapé, como client-side scanning, e nomes de órgãos e tratados internacionais, como a Convenção sobre os Direitos da Criança, quando eles encontram referência no português brasileiro. Essa opção é alinhada à missão de democratizar o acesso à informação que guia este esforço de tradução. Não traduzimos, contudo, títulos de documentos e matérias, assim como nomes de organizações sem traduções já usadas e estabelecidas no Brasil. Outros termos como stalking e bullying foram mantidos no original, visto que já se encontram disseminados dentro da esfera pública brasileira.

Por fim, agradecemos a CRIN e defenddigitalme por acreditar em nosso trabalho e apoiar esta tradução. Em especial, agradecemos a Diana Gheorghiu, Legal and Policy Officer da CRIN, com quem conversamos ao longo do ano. Este trabalho está alinhado ao compromisso do IP.rec em defender os direitos humanos em suas interações com as tecnologias digitais e com as políticas públicas e privadas que têm estruturado o desenvolvimento, aplicação e adoção dessas tecnologias. Também agradecemos à pesquisadora Marina Meira, que atuou como revisora desta tradução e nos conectou à Diana.

Assim, desejamos boa leitura e esperamos que possamos discutir de maneira séria e informada as questões apontadas neste relatório.

# Sumário executivo

O debate sobre criptografia e os direitos da criança muitas vezes é posto como uma oposição entre proteção de crianças e defesa de liberdades civis. No entanto, essa polarização esconde uma verdade mais complexa.

As crianças, seus direitos e seus interesses estão em todos os lados desse discurso. As aplicações da criptografia podem proteger ou expor crianças à violência, promover ou minar sua privacidade, incentivar ou reprimir sua expressão. A criptografia envolve quase todos os seus direitos humanos a partir de uma variedade de perspectivas.

Estamos em um ponto em que a forma como o ambiente digital é controlado, acessado e regulado definirá como as crianças se relacionarão com ele nas próximas décadas. É essencial que tal formulação de políticas se baseie em um entendimento fundamentado, no respeito pelo impacto na gama de seus direitos, e inclua de forma significativa todos aqueles cujos direitos estão em jogo. Este relatório busca explorar o tema da criptografia em toda a sua complexidade e estabelecer princípios para uma abordagem baseada nesses direitos.

## A história da criptografia

A criptografia e os debates em torno dos seus usos têm uma longa história. Para entender os desafios que existem hoje, o relatório começa oferecendo um breve panorama dessa história, desde o início das "guerras criptográficas" na década de 1970 com a classificação da encriptação como o munição sob a lei dos Estados Unidos, até o surgimento dos computadores em empresas comerciais nos anos 1980, e o uso crescente de computadores pessoais e *World Wide Web* na década de 1990. O relatório apresenta as tentativas de obter chaves que dão acesso pela "porta dos fundos" às comunicações, tais como a iniciativa *Clipper Chip*, o hacking de empresas de cartões inteligentes e as pressões governamentais sobre os serviços de correios eletrônicos criptografados. Também analisa as propostas mais recentes das agências, e as objeções a elas, de adicionar um participante silencioso em conversas e chamadas online. Neste contexto, o relatório examina os diversos impulsionadores políticos para restringir a criptografia ao longo do tempo, do combate ao terrorismo, a luta contra o crime, o suborno, a corrupção, até o enfrentamento da desinformação e da violência das massas, e o foco atual no abuso sexual infantil online.

## Entendendo a tecnologia

Desenvolver uma abordagem dos direitos da criança à criptografia requer uma compreensão profunda da tecnologia: como funciona, como é utilizada e como está integrada no ambiente digital.
O relatório explora o lugar da criptografia no ambiente digital, analisando as diversas ferramentas tecnológicas em relação aos seus usos, benefícios e comprometimentos. Ele começa com uma explicação básica sobre como a Internet funciona e de que forma a *World Wide Web* é executada nela. Em seguida, aprofunda-se em como a criptografia ajuda a criar websites seguros e mostra como a mudança para uma segurança maior dos websites cria desafios para as organizações responsáveis por desenvolver listas de websites a serem bloqueados ou monitorados. Também discute a diferença entre conteúdo e metadados, e os poderosos usos do último, especialmente quando agregados e analisados. Explora-se o argumento de que metadados podem apontar padrões que sugerem atividades ilegais, incluindo a ideia de que metadados devem ser utilizados para identificar e justificar intervenções direcionadas para lidar com abuso sexual infantil online.

Para além da confidencialidade, o relatório destaca outros usos da criptografia, como o anonimato e a autenticação, baseando-se no argumento de que a criptografia não é uma tecnologia única, sendo mais próxima a um conceito. Enfatiza-se, então, o impacto da criptografia na vida das crianças em diversas esferas, como saúde, educação e lazer, e discute as questões levantadas pelos serviços de monitoramento e controle parental.

Neste contexto, o relatório detalha tecnologias relevantes para o debate sobre criptografia e direitos da criança, particularmente aquelas usadas para identificar e remover materiais de abuso sexual infantil. Examina-se a varredura de conteúdo não encriptado para corresponder com imagens conhecidas através do exemplo do PhotoDNA e, indo além da identificação de imagens de abuso sexual infantil, aborda a expansão desse método para a área de contraterrorismo. Também destaca a escassez de informações sobre tecnologias semelhantes que seriam capazes de operar em ambientes digitais ao vivo e em tempo real. O relatório analisa então as dificuldades de identificação de comportamentos ilegais em ambientes criptografados. Ele foca na varredura pelo lado do cliente – um método de análise do conteúdo no dispositivo – e discute as diferentes opiniões dos especialistas no tema, desde a percepção vantajosa dele como um meio menos intrusivo de identificar conteúdo em comparação com o acesso a todas as comunicações do usuário, até as críticas de que cria desafios de segurança, quebra as expectativas de privacidade dos usuários e de que poderia ser reaproveitado para vigilância e censura.

O relatório então discute a criptografia homomórfica – uma tecnologia que permite operações em dados encriptados sem descriptografá-los – e outras tecnologias emergentes. Isso mostra como alguns encaram esses métodos de proteção da privacidade como uma forma de fazer o debate avançar, enquanto outros sublinham que essas tecnologias ainda não estão completamente desenvolvidas, custando caro e que ainda apresentam problemas de segurança, privacidade e jurisdicionais. O relatório, em seguida, aborda o acesso secreto a conteúdos em tempo real por meio de escuta telefônica – adicionando uma parte silenciosa às comunicações encriptadas ou explorando vulnerabilidades de segurança através de "hacking legal". Discute-se até que ponto esses métodos deveriam ser aceitáveis e sujeitos a salvaguardas, além de alertar que isso poderia levar a um constante "jogo de gato

e rato" de corrigir uma vulnerabilidade que também é explorada por agentes mal intencionados, e depois ter criado uma nova. O relatório observa a possibilidade de obter acesso oculto a conteúdos em tempo real por meio de malware e interceptação, por exemplo, com um software como o "Pegasus". As explicações em torno da tecnologia terminam com o argumento de que a criptografia, se não na prática, pode ser quebrada em seu princípio, caso seus objetivos sejam comprometidos. O relatório também discute a denúncia de usuários e conclui que ela pode ser implementada sem representar riscos para a privacidade e a segurança em ambientes criptografados, embora as denúncias de usuários necessitem de respostas adequadas e em tempo hábil das plataformas.

## Atritos e falhas: a busca por consenso

O debate sobre criptografia já foi descrito como "termonuclear", com "emoções intensas em ambos os lados". Para ir além das divisões que existem atualmente em relação à criptografia, é necessário compreender os atritos, fraturas e falhas que existem neste espaço, bem como onde há margem para consenso.

O relatório explora as diversas perspectivas adotadas nas discussões atuais. Essas perspectivas foram extraídas da revisão da literatura, bem como de entrevistas, questionários e conversas com toda a gama de organizações e especialistas que trabalham nessa área, incluindo proteção infantil, direitos da criança, direitos digitais, privacidade e proteção de dados, regulação da Internet e setor de tecnologia.

O relatório explora vários temas, mapeando áreas de concordância e divergência para entender o debate e ajudar o diálogo a avançar. Identificaram-se várias áreas de consenso, incluindo uma concordância fundamental de que o abuso e a exploração sexual de crianças online exigem ação urgente. O ponto em que os entrevistados discordaram foi sobre a melhor forma de atingir esse objetivo enquanto se protege os direitos humanos. Uma ampla gama de especialistas descreveu a natureza altamente emocional do debate, que corre o risco de impedir o envolvimento de outras áreas, embora alguns tenham sentido que progresso está sendo feito. Outra dificuldade é o excesso de confiança em números específicos sobre a escala do abuso sexual infantil online. Participantes de diferentes lados do espectro argumentaram, por diferentes motivos, que esses números não refletem verdadeiramente a natureza e a extensão do problema. Por um lado, os crimes de abuso sexual infantil são subnotificados. Esse é um problema específico à luz da tendência emergente de sextorsão, uma combinação de crime de colarinho branco e exploração sexual infantil, pois as plataformas digitais de pagamento não relatam atividades financeiras como abuso sexual. Por outro lado, certas denúncias contêm partes duplicadas de conteúdos e imagens compartilhadas consensualmente entre adolescentes. Mais importante ainda, está longe de ser claro até que ponto as denúncias de material de abuso sexual infantil online levam a investigações e prisões de infratores e à proteção de crianças.

Os entrevistados também concordaram que a regulação online não deve ser tratada como uma questão de "privacidade versus proteção", ou "privacidade dos adultos versus proteção das crianças", mas que deve haver uma conversa equilibrada sobre todos os direitos humanos envolvidos. Alguns defensores dos direitos da criança consideram a atual polarização como uma falha geral no discurso sobre as crianças, que as vê como "objetos de proteção em vez de sujeitos de direitos plenamente formados". Eles também defenderam uma melhor compreensão de como a privacidade afeta o desenvolvimento infantil. Muitos participantes enfatizaram que a privacidade permite o exercício de outros direitos, inclusive a proteção contra a violência. Mas alguns advertiram que a criptografia não deve ser vista como totalmente benéfica para a proteção da privacidade, uma vez que a privacidade das pessoas que sofreram abuso sexual não recebe atenção suficiente.

Uma preocupação relacionada foi o fato de não ser dada ênfase suficiente à segurança. Vários entrevistados chamaram a atenção para exemplos de culpabilização da vítima, especialmente no uso casual da linguagem. Há um consenso claro de que os sobreviventes de abuso sexual infantil devem ser incluídos de forma significativa nos processos de reforma, mas não devem ser feitas presunções sobre suas opiniões, pois são um grupo diverso com experiências e perspectivas variadas.

Também houve concordância entre os entrevistados de que a tecnologia é um tópico central na abordagem da questão do abuso sexual infantil online. Enquanto alguns argumentaram que a tecnologia facilita o abuso direta e indiretamente, e, portanto, soluções técnicas devem ser desenvolvidas, outros alertaram contra o "tecnossolucionismo". Eles enfatizaram que diferentes opções de políticas, algumas de natureza tecnológica e outras não, podem ser usadas para alcançar diferentes resultados. Portanto, o ponto de partida deve ser o objetivo a ser alcançado, e não os méritos de uma tecnologia específica.

A questão de quem tem um papel legítimo na implantação da tecnologia também foi um tema comum nas entrevistas. Alguns participantes sugeriram a utilização das capacidades existentes de investigação por meio de tecnologia das autoridades responsáveis pela aplicação da lei – embora tenha sido levantada uma objeção de que a escala do abuso representa um desafio. Outros questionaram se as forças de aplicação da lei deveriam se basear na narrativa do "perigo estranho" para utilizar ferramentas automatizadas em escala. Outros ainda foram além e alertaram que, devido ao investimento insuficiente, a capacidade das forças de segurança de lidar com o abuso sexual infantil online se deteriorou. Alguns também alertaram contra o sequestro de função por forças policiais. Essa era uma preocupação, especialmente em relação às crianças de comunidades desfavorecidas e marginalizadas, que têm maior probabilidade de ter experiências negativas com o policiamento.

Em vista dessas limitações da tecnologia e de quem deve usá-la, alguns entrevistados demandaram uma abordagem sistêmica para o abuso sexual infantil online. Como medidas tecnológicas, eles sugeriram pequenos ajustes cumulativos com relação ao design do sistema e dos serviços. De um modo mais geral, argumenta-

ram que é necessário, embora talvez seja menos conveniente politicamente, concentrar-se nos outros atores no ecossistema mais amplo em vez de procurar a bala de prata tecnológica. Eles defenderam mais investimentos em escolas e educação, serviços de saúde e serviços sociais, especialmente aqueles que ajudam os sobreviventes em sua recuperação.

Houve um consenso sobre a necessidade de supervisão democrática na forma de regulação das plataformas. Os entrevistados argumentaram a favor de mais consistência e responsabilidade, com orientações claras sobre o que se espera das empresas e como elas devem proceder. No entanto, os participantes divergiram sobre onde colocar o peso da ação. Alguns consideraram que as ferramentas criadas pelas plataformas beneficiam as forças de aplicação da lei, enquanto outros alertaram contra a dependência de "ferramentas monopolísticas" criadas por "atores politicamente irresponsáveis" e a privatização das funções das forças de segurança.

Muitos entrevistados ressaltaram que o debate é anglo e eurocêntrico, além de enfatizarem que leis não podem ser simplesmente transplantadas de uma jurisdição para outra, mas devem ser adaptadas ao contexto nacional. Por exemplo, alguns destacaram desafios específicos enfrentados fora da Europa e da América do Norte, como a discriminação por design e o uso de dispositivos de baixo custo.

## O impacto da criptografia nos direitos das crianças

O relatório aplica uma abordagem dos direitos da criança às perspectivas ricas e complexas identificadas. A Convenção das Nações Unidas sobre os Direitos da Criança é tratada como a diretriz acordada internacionalmente, que abrange a gama completa de direitos das crianças e analisa os benefícios e os riscos que as aplicações de criptografia podem representar para os direitos da Convenção. Descarta-se a oposição "privacidade versus proteção", mostrando que não é certo afirmar que a criptografia oferece apenas benefícios para a privacidade e apenas riscos para a proteção das crianças.

Os canais criptografados podem ser usados para fazer circular materiais de abuso sexual de crianças, o que viola a privacidade das vítimas. Ao mesmo tempo, os canais criptografados podem ser usados para se comunicar de forma segura com o mundo exterior e buscar ajuda quando crianças são vítimas de violência perpetrada, por exemplo, por um membro da família. Além disso, a criptografia envolve não apenas o direito das crianças à privacidade e à proteção contra a violência, mas também à não discriminação, o direito à vida, liberdade de pensamento, consciência e religião, o direito à saúde e até mesmo a proteção de crianças afetadas por conflitos armados. O relatório analisa detalhadamente o direito à privacidade e as suas restrições admissíveis como um exemplo de como lidar com a regulação e com as tensões na aplicação dos direitos das crianças.

Indo além da "privacidade versus proteção", o relatório explora como o impacto da criptografia varia de acordo com o histórico, as necessidades e as identidades das crianças, especialmente quando elas fazem parte de grupos desfavorecidos ou marginalizados. Os casos buscam enfatizar a capacidade das crianças de exercerem seus direitos em uma ampla variedade de contextos.

Em relação ao Estado, o relatório examina o papel da criptografia para crianças que são politicamente ativas, mas que vivem sob regimes repressivos, crianças ativistas e que fazem denúncias, bem como para crianças que querem tomar decisões sobre seu próprio corpo (por exemplo, em relação ao aborto) e aquelas cujos direitos são restringidos pela lei geral de direitos humanos (por exemplo, sob estados de emergência ou para a proteção da segurança nacional). Em relação à família, o relatório analisa o impacto da criptografia para crianças cujos interesses ou pontos de vista são diferentes dos pais, e crianças que podem ser colocadas em situação de desvantagem devido ao status de seus pais. Em relação às empresas, os casos se concentram no impacto desproporcional que as plataformas podem ter sobre os direitos das crianças, especialmente quando as plataformas são extremamente influentes ou coletam metadados de crianças.

## Propostas legislativas

Nos últimos anos, houve um aumento no número de propostas de legislação e outras iniciativas relacionadas ao ambiente digital que afetam a criptografia, muitas vezes com o objetivo de manter as pessoas seguras.

O relatório apresenta um breve panorama de três dessas propostas que foram apresentadas nos Estados Unidos (o *EARN IT Act* de 2022), no Reino Unido (o *Online Safety Bill*) e na União Europeia (a proposta de Regulamento que estabelece regras para prevenir e combater o abuso sexual infantil). Seus intuitos de proteger as crianças online, particularmente contra o abuso e a exploração sexual, são incontroversos. No entanto, o relatório apresenta importantes áreas de divergência no que diz respeito ao impacto dessas propostas na criptografia e nos direitos das crianças.

## Uma abordagem do direito das crianças à criptografia: Princípios para os formuladores de políticas públicas

A efetivação da totalidade dos direitos das crianças em ambientes digitais é complexa e cheia de nuances. Não existem soluções únicas para todos os problemas. Este relatório apresenta um conjunto de recomendações baseadas em princípios para regulações futuras que respeitem os direitos das crianças.

Por fim, o relatório estabelece dez princípios que orientam uma abordagem pautada nos direitos das crianças em relação à criptografia. Tanto o enquadramento da questão quanto o resultado final das diretrizes políticas são importantes, portanto, os cinco primeiros princípios tratam de questões de processo, enquanto os cinco últimos dizem respeito à composição da formulação de políticas.

## Processo

**1. As ações que afetam o ambiente digital devem respeitar a gama completa de direitos das crianças, desde a proteção contra a violência até a privacidade e a liberdade de expressão.**

- As discussões precisam ir além da polarização "privacidade versus proteção" e reconhecer que todos os direitos das crianças são igualmente importantes e se apoiam mutuamente.
- Todas as intervenções que tenham um impacto significativo nas crianças devem se basear em avaliações de impacto sobre os direitos da criança.

**2. Nenhuma lei, política ou tecnologia isolada pode proteger as crianças online ou garantir seus direitos humanos de forma mais ampla. As intervenções que envolvem criptografia devem ser vistas dentro de um ecossistema mais amplo com vários atores.**

- A criptografia não deve ser o ponto de partida nas discussões sobre diretrizes políticas. Em vez disso, os formuladores de políticas públicas devem primeiro identificar os objetivos a serem alcançados e, em seguida, considerar uma série de soluções, tecnológicas ou não, levando em consideração a variedade de atores envolvidos no ecossistema social.
- As partes interessadas devem ser cautelosas com soluções tecnológicas que sirvam para todos.
- O sistema completo de proteção à criança, desde as forças de segurança e o sistema judiciário até os serviços sociais e a reabilitação das vítimas, deve ser apoiado.

**3. Todos aqueles com conhecimentos relevantes (por exemplo, em proteção infantil, regulação da tecnologia e da Internet, proteção de dados e privacidade, direitos humanos em geral etc.) devem estar envolvidos nas discussões e na tomada de decisões relacionadas a crianças e ao ambiente digital, inclusive sobre criptografia.**

- Deve-se dar atenção especial à abordagem e à linguagem utilizada.
- Deve-se dar mais ênfase à importância de dados precisos.

**4. Crianças e outras comunidades diretamente afetadas, por exemplo, sobreviventes de abuso sexual infantil ou aqueles desproporcionalmente afetados por práticas intrusivas de dados, devem ser ouvidas e seus pontos de vista devem receber o devido valor.**

**5. O ambiente digital é interconectado e é muito provável que a regulamentação em uma jurisdição cause efeitos em cascata em outras, portanto, os formuladores de políticas envolvidos com a criptografia devem considerar o impacto além de sua própria jurisdição.**

## Composição

**6. Não deve haver proibição generalizada da criptografia para crianças.**

**7. Intervenções que envolvem criptografia devem considerar e abordar contextos políticos, econômicos, sociais e culturais específicos.**

- Os participantes do debate devem promover uma melhor compreensão da ampla gama de usos do ambiente digital, especialmente para além dos contextos anglo e eurocêntricos.
- As partes interessadas devem reconhecer que a tecnologia pode ser reaproveitada para promover uma variedade de objetivos políticos, incluindo a vigilância e a identificação de material legítimo.

**8. As restrições aos direitos fundamentais relativos das crianças, como à privacidade, devem ser necessárias e proporcionais. Elas devem ser suficientemente claras e precisas, limitadas à concretização de um objetivo legítimo e à forma menos intrusiva de atingi-lo.**

**9. A elaboração de políticas públicas deve abordar o papel das empresas.**

- Quando as empresas tiverem conhecimento de conteúdo ilegal em seus serviços, deverão informar imediatamente as autoridades.
- As empresas devem publicar relatórios de transparência sobre como previnem e corrigem violações dos direitos das crianças em seus serviços.

**10. As crianças devem ter acesso à justiça para todas as violações de sua gama completa de direitos no ambiente digital, inclusive quando a criptografia está envolvida. Devem ser disponibilizados mecanismos de reclamação gratuitos, eficazes e adequados para as crianças, juntamente com mecanismos de supervisão independentes.**

- A denúncia do usuário deve ser confidencial, segura e adequada para crianças, e mecanismos de "sinalizador confiável" devem ser considerados.
- Resultados inadvertidos devido a erros de processos automatizados devem ser reversíveis por meio de suporte humano.

# Introdução

A criptografia está em toda parte. Quando você navega em um site seguro, se comunica por meio de um aplicativo de mensagens, acessa serviços bancários *online* ou confia seus dados a um serviço de saúde *online*, está contando com a criptografia. Tanto crianças quanto adultos dependem da criptografia para preservar a segurança de suas informações pessoais e comunicações, de forma *online* ou *offline.*

O debate sobre criptografia e os direitos das crianças muitas vezes é enquadrado a partir da divisão entre uma abordagem de proteção infantil e um foco nas liberdades civis. No entanto, essa polarização esconde uma verdade mais complexa.

As crianças, seus direitos e seus interesses estão em todos os lados desse discurso. As aplicações da criptografia podem proteger ou expor crianças à violência, promover ou minar sua privacidade, incentivar ou reprimir sua expressão. A criptografia envolve quase todos os seus direitos humanos a partir de uma variedade de perspectivas.

Além disso, o impacto que a criptografia tem, seja positivo ou negativo, também pode variar significativamente de criança para criança, dependendo de suas origens, necessidades e identidades. Portanto, se a abordagem à criptografia pretende verdadeiramente levar todos os direitos das crianças a sério, ela deve levar em consideração como crianças são afetadas em todo o globo, incluindo as experiências específicas de crianças pertencentes a comunidades desfavorecidas e marginalizadas.

## Rumo a uma abordagem de direitos das crianças à criptografia

Este relatório tem como objetivo reconhecer a complexidade dos impactos da criptografia na vida das crianças e estabelecer uma abordagem que leve em consideração todos os aspectos de seus direitos.

O desenvolvimento da criptografia está intrinsecamente relacionado com os avanços tecnológicos do final do século XX e, especificamente, da Internet. Para entendermos onde estamos agora, precisamos entender como chegamos até aqui. Com isso em mente, o relatório começa com a história do debate em torno da criptografia, desde as "guerras criptográficas" da década de 1970, até os desafios que enfrentamos hoje.

Em resposta à necessidade de uma análise acessível sobre essa tecnologia, o relatório explora o conceito de criptografia e seu funcionamento. Isso inclui uma análise das tecnologias utilizadas para identificação de material de abuso sexual infantil *online*, bem como para combater a exploração e o abuso sexual *online*. Nosso objetivo é esclarecer os benefícios, custos e comprometimentos envolvidos no uso dessa tecnologia, para que seu papel legítimo possa ser avaliado.

Para superarmos as divisões que existem atualmente neste campo, devemos entender as fricções e as falhas que existem neste espaço, bem como onde há espaço para consenso. Nesse sentido, o cerne da pesquisa se baseou em uma série de entrevistas com uma ampla gama de organizações e especialistas envolvidos nessa questão. O relatório apresenta e examina uma variedade de perspectivas e abordagens adotadas por aqueles que trabalham em questões relacionadas à criptografia, a fim de ajudar a superar a polarização que tem sido tão presente no debate sobre criptografia.

Com base nesse contexto, exploramos como a criptografia se relaciona com os direitos das crianças, tratando a Convenção das Nações Unidas sobre os Direitos da Criança como um referencial internacional aceito e avaliando como ela se aplica às crianças afetadas por ou que usam tecnologias que envolvem criptografia. Esta análise aborda as tensões que podem surgir entre a proteção das crianças contra a violência e a preservação de sua privacidade, assim como a privacidade do público em geral. Concluímos que é necessário ir além de uma abordagem de privacidade versus proteção se quisermos garantir que todos os direitos das crianças sejam protegidos.

## Moldando o espaço *online* para as crianças nas próximas décadas

Por fim, com este relatório, apresentamos nossa perspectiva sobre o assunto e estabelecemos princípios que orientam uma abordagem pautada nos direitos das crianças em relação à criptografia. O objetivo é fornecer uma base sólida para a elaboração e avaliação de políticas sobre essa questão, priorizando os direitos das crianças.

Estamos em um momento em que a forma como o espaço digital é controlado, acessado e regulado moldará como as crianças vão interagir com ele nas próximas décadas. Portanto, é fundamental que as políticas formuladas nesse contexto sejam baseadas em uma compreensão informada de seu impacto sobre os direitos das crianças, bem como sobre os direitos de todos aqueles envolvidos.

# Metodologia

Esta pesquisa centrou-se no impacto da criptografia sobre o direito das crianças, particularmente no contexto do debate atual sobre criptografia e exploração e abuso sexual infantil *online*. O relatório é baseado em revisão de literatura, bem como em entrevistas semi estruturadas e conversas informais[1] com especialistas que trabalham com este tópico, e em respostas escritas fornecidas a um questionário.

A revisão de literatura mirou zonas específicas de concordância e discordância entre os participantes do debate, e as fontes foram identificadas por meio de pesquisa secundária e recomendações de profissionais que trabalham na área. A revisão de literatura embasou algumas das análises do relatório e também foi usada para estruturar a abordagem das entrevistas. Os entrevistados eram representantes de diversas esferas, incluindo proteção infantil, direitos das crianças, direitos digitais, privacidade e proteção de dados, regulação da Internet e setor de tecnologia.

Adultos sobreviventes de exploração e abuso sexual infantil *online* também foram entrevistados. Para levar em consideração as perspectivas das crianças sobre essa questão, foi feita referência a literatura que cita estudos realizados por pesquisadores que trabalham diretamente com esses grupos.

Além das entrevistas semiestruturadas, o relatório se baseia em conversas informais que, na maioria dos casos, não foram estruturadas. Questionários foram enviados a várias organizações e abordavam questões semelhantes às das entrevistas. Com os questionários, a intenção era incluir organizações fora dos espaços dominantes anglo e eurocêntricos e dar a elas a oportunidade de fornecer informações em um formato flexível. Quando os participantes concordaram, as opiniões individuais foram diretamente atribuídas a eles, a fim de aumentar a transparência do debate, transmitir sua riqueza e ajudar a traçar um caminho a ser seguido.

Gostaríamos de agradecer a todos os entrevistados e respondentes do questionário que nos deram seu tempo para participar da pesquisa para este relatório, bem como todos os nomeados e anônimos que revisaram ou forneceram comentários às versões rascunho.

Falar, compartilhar e ouvir palavras de reconhecimento mútuo é uma etapa importante na criação de relacionamentos colaborativos, responsáveis, contínuos e respeitosos entre as comunidades que ocupam diferentes territórios no cenário compartilhado deste debate.

Os autores são gratos à natureza aberta e solidária da ampla gama de comentários de pessoas e organizações que recebemos, em particular aqueles que sofreram

1 N.T. Optamos por traduzir a expressão "background conversations" como "conversas informais" na maior parte das suas ocorrências.

abuso sexual e violência na infância, e aqueles que trabalham no apoio às vítimas e sobreviventes, bem como especialistas em criptografia, em política, de instituições, da sociedade civil, do mundo acadêmico e do setor de tecnologia.

Fizemos o nosso melhor para representar com precisão as perspectivas dos outros, mas o relatório e quaisquer erros fora das citações diretas são, em última análise, opinião e responsabilidade dos autores.

## Lista pública de entrevistados

| | Representative | Organisation |
|---|---|---|
| 1. | Duncan McCann e Izzy Wick | 5Rights Foundation |
| 2. | Maria Góes de Mello e<br>João Francisco de Aguiar Coelho | Instituto Alana |
| 3. | Iverna McGowan Smyth | Centre for Democracy and Technology (Sede Europeia) |
| 4. | Um representante | Coram International -<br>Coram Children's Legal Centre |
| 5. | Amy Crocker e Isaline Wittorski | ECPAT |
| 6. | Joe Mullin | Electronic Frontier Foundation (EFF) |
| 7. | Tom Fredrik Blenning | Electronic Frontier Norway |
| 8. | Ella Jakubowska | European Digital Rights (EDRi) |
| 9. | Hosein Badran | Internet Society (ISOC) |
| 10. | Daniel Sexton e Michael Tunks | Internet Watch Foundation (IWF) |
| 11. | Rhiannon-Faye McDonald e<br>Victoria Green | Marie Collins Foundation |
| 12. | Gail Kent e Helen Charles | Meta |
| 13. | Yiota Souras e Jennifer Newman | National Center for Missing & Exploited Children (NCMEC) |
| 14. | Dianne Ludlow | One in Four |
| 15. | Caroline Wilson Palow | Privacy International |
| 16. | Chloe Setter | WeProtect Global Alliance |
| 17. | Ian Brown | Em caráter pessoal |
| 18. | Wendy M. Grossman | Em caráter pessoal |
| 19. | Richard Wingfield | Em caráter pessoal |



Somos gratos também aos representantes das seguintes organizações, que forneceram respostas por escrito ao nosso questionário:

- Africa Media and Information Technology Initiative (AfriMITI)
- Alexander von Humboldt Institute for Internet and Society
- Bits of Freedom
- Associação Data Privacy Brasil de Pesquisa.

Também agradecemos a outros participantes que trabalham nessa área que ofereceram contribuições durante aproximadamente 15 horas de conversas privadas.

Estendemos os convites a outras partes interessadas que trabalham no setor, incluindo forças de segurança e o setor de caridade. No futuro, esperamos poder nos conectar com aqueles que não puderam participar desta pesquisa.

# Criptografia: Uma breve história

A criptografia não é algo novo, tampouco é o debate sobre sua aplicação e regulamentação. As discussões sobre políticas públicas relacionadas à criptografia atualmente se concentram nos desafios que ela impõe à identificação e prevenção da exploração sexual e do abuso infantil *online*. Contudo, esse é apenas o capítulo mais recente de um longo debate. Compreender a história da criptografia é fundamental para decifrar as tensões e desacordos que persistem nos dias de hoje.

## A história

O desejo dos Estados de controlar a criptografia - as técnicas para comunicação segura na presença de destinatários não intencionados - tem raízes antigas. Entre os sistemas estatais mais conhecidos e as tentativas de quebrar os do outro lado, estão aqueles usados durante a Segunda Guerra Mundial para habilitar e decifrar segredos de Estado entre si, usando conhecimento sobre o que o outro lado estava planejando em uma guerra de informações.

Após a Segunda Guerra Mundial, os Estados Unidos (EUA), Reino Unido, Austrália, Canadá e Nova Zelândia formaram uma aliança chamada Five Eyes, com base em uma série de acordos bilaterais de vigilância e compartilhamento de inteligência. Tais acordos permitiram que esses países compartilhassem inteligência coletada e decifrada por suas agências de inteligência por padrão. Embora os acordos subjacentes da Five Eyes não estejam em domínio público, a preocupação entre os críticos é que o envolvimento de agências de inteligência estrangeiras no compartilhamento de informações de inteligência permita às agências domésticas obter informações que não poderiam acessar sem violar restrições legais nacionais sobre vigilância estatal.[2]

À medida que avanços tecnológicos aceleraram, as "guerras criptográficas" ganharam destaque na década de 1970, quando o governo dos EUA tentou classificar a criptografia como uma tecnologia de armamento - uma tecnologia reconhecida e regulamentada como uma arma de guerra. As origens da securitização e o desejo dos Estados de controlar o ciberespaço estavam presentes desde o início e são parte importante para entender por que há críticas generalizadas a qualquer proposta que enfraqueça ou busque proibir o uso da criptografia hoje.

2 Veja: https://privacyinternational.org/learn/five-eyes

Nos primórdios da expansão da Internet comercial, a criptografia era uma tecnologia que as empresas nos EUA podiam escolher usar em produtos que construíam e exportavam. No entanto, o governo dos EUA promulgou legislações restritivas ao uso da criptografia, tanto em termos de controles de exportação, impedindo a exportação de produtos físicos e de *software* que empregassem criptografia forte para mercados fora dos EUA, quanto criando requisitos domésticos para permitir o acesso estatal ao conteúdo digital de comunicações.

À medida que o debate nos EUA crescia sobre como cobrar pela telefonia[3] nos estágios iniciais da Internet, uma variedade maior de políticos e governos se envolvia devido às implicações econômicas e preocupações sobre soberania nacional.

A autora Wendy Grossman previu, em 1997, que o entusiasmo tecnológico do "Vale do Silício" que impulsionava a afirmação de que o novo meio de comunicação iria "remodelar o mundo, minar o status quo e eliminar governos nacionais e corporações multinacionais" inevitavelmente levaria à imposição de governança e controles estatais. Mesmo então, quase trinta anos atrás, quando a maioria das pessoas ainda não estava *online*, esses controles estavam sendo discutidos como uma governança que moldaria a Internet de acordo com a ideia dos políticos do que seria "seguro".[4]

Essa definição de "segurança" *online* era controversa mesmo naquela época. Afinal, segurança para quem e contra o quê?

Na década de 1980, como explica o site Crypto Museum[5], quando os computadores estavam começando a surgir em empresas comerciais depois de serem exclusivos de ambientes militares, tornou-se cada vez mais necessário que as ligações sem fio e com fio transportassem não apenas os dados de um único computador, mas pacotes de dados completos de vários dispositivos simultaneamente, com frequência incluindo voz e dados de fax. Tais dispositivos são conhecidos como "cifradores em massa". Esses equipamentos eram volumosos e requeriam intervenções manuais, como ligar e desligar a criptografia, ou o uso de um dispositivo eletrônico para a distribuição de variáveis criptográficas, como chaves criptográficas.

3 A telefonia é uma tecnologia associada à comunicação interativa entre duas ou mais partes fisicamente distantes por meio da transmissão eletrônica de voz ou outros dados: https://www.techtarget.com/searchunifiedcommunications/definition/Telephony

4 Grossman, W., *net.wars*, 1997, New York University Press, p. 196, https://nyupress.org/9780814731031/net-wars

5 Veja: https://www.cryptomuseum.com/crypto/index.htm



Durante a década de 1990, a World Wide Web impulsionou a expansão do acesso à informação para o público geral via Internet. Essa década também viu o surgimento do comércio eletrônico e o advento da criptografia "fácil" em grande escala pelos entusiastas tecnicamente capacitados, por meio do Pretty Good Privacy (ou PGP, como é conhecido). Tal ferramenta permitia aos usuários se comunicarem de forma segura, criptografando e descriptografando mensagens, autenticando mensagens por meio de assinaturas digitais e criptografando arquivos. Com o aumento do uso do computador pessoal, o governo dos EUA tentou criar uma rota física para permitir que o governo sempre tivesse acesso a uma chave para comunicações criptografadas, usando o chamado Chip Clipper, que possibilitaria o acesso de "porta dos fundos" às comunicações de quaisquer dispositivos equipados com o chip. O processo envolvia a entrega de chaves criptográficas a uma terceira parte, que só as disponibilizaria às agências governamentais após a obtenção de autorização para interceptar uma comunicação específica. As forças policiais e as agências que desejavam acesso ao conteúdo da mensagem poderiam, então, abordar a terceira parte sem notificar o proprietário da chave.

Como reação à ameaça de proibição da criptografia pelo governo dos EUA, foram lançados vários pacotes públicos robustos de criptografia, incluindo Nautilus, PGP e PGPfone. Acreditava-se que, ao tornar a criptografia forte amplamente disponível ao público, o governo não conseguiria impedir seu uso. Essa abordagem se mostrou eficaz e, apesar de uma falha que comprometeu sua segurança, a vida do Clipper Chip foi limitada, encerrada em 1994.

Essas propostas de políticas governamentais geraram controvérsias recorrentes. Wendy Grossman disse em entrevista para este relatório: "Não é surpreendente que a Internet se sinta ameaçada? Não é surpreendente que essa sensação de ameaça una a comunidade, e que alguns elementos se unam com determinação para garantir que tentativas de regulamentação falhem? Regular o ciberespaço é muito parecido com atirar no mensageiro".[6]

Em 1999, houve consenso entre os tecnólogos e políticos que defendiam princípios libertários de livre mercado de que a imposição de controles de exportação significava que os EUA exportavam dispositivos que não eram tão seguros quanto deveriam ser. Matt Blaze, que expôs as deficiências do Chip Clipper[7] em seu extenso trabalho em criptografia, descreveu esse período como um em que "a 'criptografia' [foi] erroneamente difamada como uma espécie de ferramenta criminosa no exato momento em que deveríamos estar integrando uma segurança robusta na infraestrutura da Internet" e que isso atrasou a segurança da Internet "em pelo

6 CRIN e entrevista ddm com Wendy M. Grossman, 28 de setembro de 2022

7 CCallas, J., A Tentativa Recente de Quebrar a Criptografia é uma Ideia Antiga Provada Errada, 23 de julho de 2019, https://www.aclu.org/news/privacy-technology/recent-ploy-break-encryption-old-idea-proven-wrong

menos uma década, e ainda estamos pagando o preço em forma de violações regulares de dados, muitas das quais poderiam ter sido evitadas se uma melhor segurança tivesse sido incorporada desde o início".[8]

Após a tentativa de criar essas chaves que dariam acesso de "porta dos fundos" à tecnologia exportada ter falhado, as agências serviços de segurança tentaram outro método: infiltrar-se em empresas que fabricavam cartões SIM seguros para dispositivos móveis. O delator Edward Snowden, que trabalhava para a Agência de Segurança Nacional dos EUA (NSA), revelou documentos em 2015 que supostamente mostram que a NSA e seu equivalente britânico, o GCHQ, invadiram a empresa franco-holandesa de cartões inteligentes chamada Gemalto para adquirir as chaves criptográficas de milhões de cartões SIM de telefones celulares.[9] Não se sabe quantas chaves foram roubadas ou quão eficiente seria a aplicação dessas chaves, mas essa operação potencialmente permitiria acesso aos usuários de tais cartões SIM, principalmente em ambientes nos quais predominam redes 2G, como é o caso do Paquistão.

No entanto, especialistas em criptografia, defensores dos direitos digitais e empresas de tecnologia concordam que não há uma "porta dos fundos" segura para a criptografia.

> *"Qualquer 'porta dos fundos' criaria mais riscos de segurança, inclusive para usuários individuais, do que resolveria. Qualquer atrito na cadeia de transmissão de mensagens ou vulnerabilidades de segurança no protocolo de encriptação correm o risco de serem explorados por adversários (estatais e não estatais)."*[10]

Se uma "porta dos fundos" é criada para fornecer "acesso excepcional" para a aplicação da lei, é uma "porta dos fundos" para que qualquer terceiro possa acessar os conteúdos das comunicações. Isso pode parecer inofensivo, mas os resultados podem ser desastrosos, de acordo com a Internet Society.[11]

A Electronic Frontier Foundation apontou que o governo dos EUA não tem hesitado em buscar acesso a comunicações criptografadas, pressionando as empresas a facilitar a obtenção de dados a partir de mandados e a entregar dados voluntariamente.

8 Blaze, M., A Busca Exaustiva Mudou, 7 de julho de 2018, https://www.mattblaze.org/blog/newaddress/

9 Consulte o site Crypto Museum sobre a Gemalto: https://www.cryptomuseum.com/manuf/gemalto/index.htm

10 Tech Against Terrorism, Terrorist Use of E2EE: State of Play, Misconceptions, and Mitigation Strategies, 2021, https://www.techagainstterrorism.org/wp-content/uploads/2021/09/TAT-Terrorist-use-of-E2EE-and-mitigation-strategies-report-.pdf

11 ISOC, Breaking Encryption Myths: What the European Commission's leaked report got wrong about online security, 2020, https://www.internetsociety.org/resources/doc/2020/breaking-the-myths-on-encryption/



Entretanto, os EUA enfrentariam sérios problemas constitucionais se quisessem aprovar uma lei que exigisse a varredura e a notificação de conteúdo sem mandado.[12]

Apenas uma década atrás, a Lavabit, um serviço de webmail criptografado de código aberto fundado em 2004 suspendeu suas operações, em 8 de agosto de 2013, depois que o governo federal dos EUA ordenou que ela entregasse suas chaves privadas da Secure Sockets Layer para permitir que o governo espionasse os e-mails de Edward Snowden.

As novas propostas de agências incluíram discussões bem mais transparentes. As propostas mais recentes avançaram para novos pontos no processo de interceptação ou denúncia de conteúdo reconhecido. Mas o princípio permanece o mesmo: possibilitar que terceiros interceptem ou denunciem o usuário a terceiros.

A proposta seguinte do GCHQ, em 2019, era permitir que as forças da lei e agências de inteligência acessassem sistemas de mensagens privadas, adicionando um participante silencioso – usuários "fantasmas" das forças da lei ou das agências de segurança - em chats e chamadas *online*, incluindo aqueles realizados por meio de ferramentas de mensagens criptografadas, como WhatsApp, iMessage ou Signal. A "proposta fantasma"[13] foi amplamente condenada em 2019, inclusive pela Internet Society,[14] como a mais recente tentativa de um governo de contornar e/ou criar "porta dos fundos" em comunicações criptografadas, que remetia aos objetivos do Clipper Chip. Uma coalizão de mais de cinquenta organizações da sociedade civil, empresas de tecnologia e especialistas em cibersegurança, incluindo Apple, Microsoft, Human Rights Watch e Privacy International, redigiu uma objeção às propostas que poderiam "abrir as portas para abusos de vigilância que não são possíveis hoje."[15] Isso não apenas criaria vulnerabilidades no presente, como também exigiria que as empresas mantivessem essas vulnerabilidades em aberto, e não "consertassem" essa fraqueza, que então poderia ser explorada por outros.[16] Ao inserir ferramentas de vigilância em produtos, os Estados efetivamente limitariam a inovação em segurança, assim como foi visto como resultado dos controles de exportação do governo dos EUA na década de 1990.

12 EFF, If You Build It, They Will Come: Apple Has Opened the Backdoor to Increased Surveillance and Censorship Around the World, 2021, https://www.eff.org/deeplinks/2021/08/if-you-build-it-they-will-come-apple-has-opened-backdoor-increased-surveillance

13 Levy, I. and Robinson, C., *Principles for a More Informed Exceptional Access Debate*, 2018, https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate

14 ISOC, *Ghost Protocol Fact Sheet*, 2020, https://www.internetsociety.org/wp-content/uploads/2020/03/Ghost-Protocol-Fact-Sheet.pdf

15 Clayton Rice, K.C., *The Ghost Key Proposal*, https://www.claytonrice.com/the-ghost-protocol/

16 Green, M., *On Ghost Users and Messaging Backdoors*, 2018, https://blog.cryptographyengineering.com/2018/12/17/on-ghost-users-and-messaging-backdoors/

## Aonde isso nos trouxe hoje

Entender as origens das "guerras cibernéticas" e os debates de longa data sobre a vigilância estatal, além de seus efeitos relacionados aos indivíduos e à coletividade, pode ajudar de alguma forma a compreender as tensões atuais, mostrando por quais razões as soluções tecnológicas utilizadas e as abordagens políticas propostas chegaram a um certo impasse.

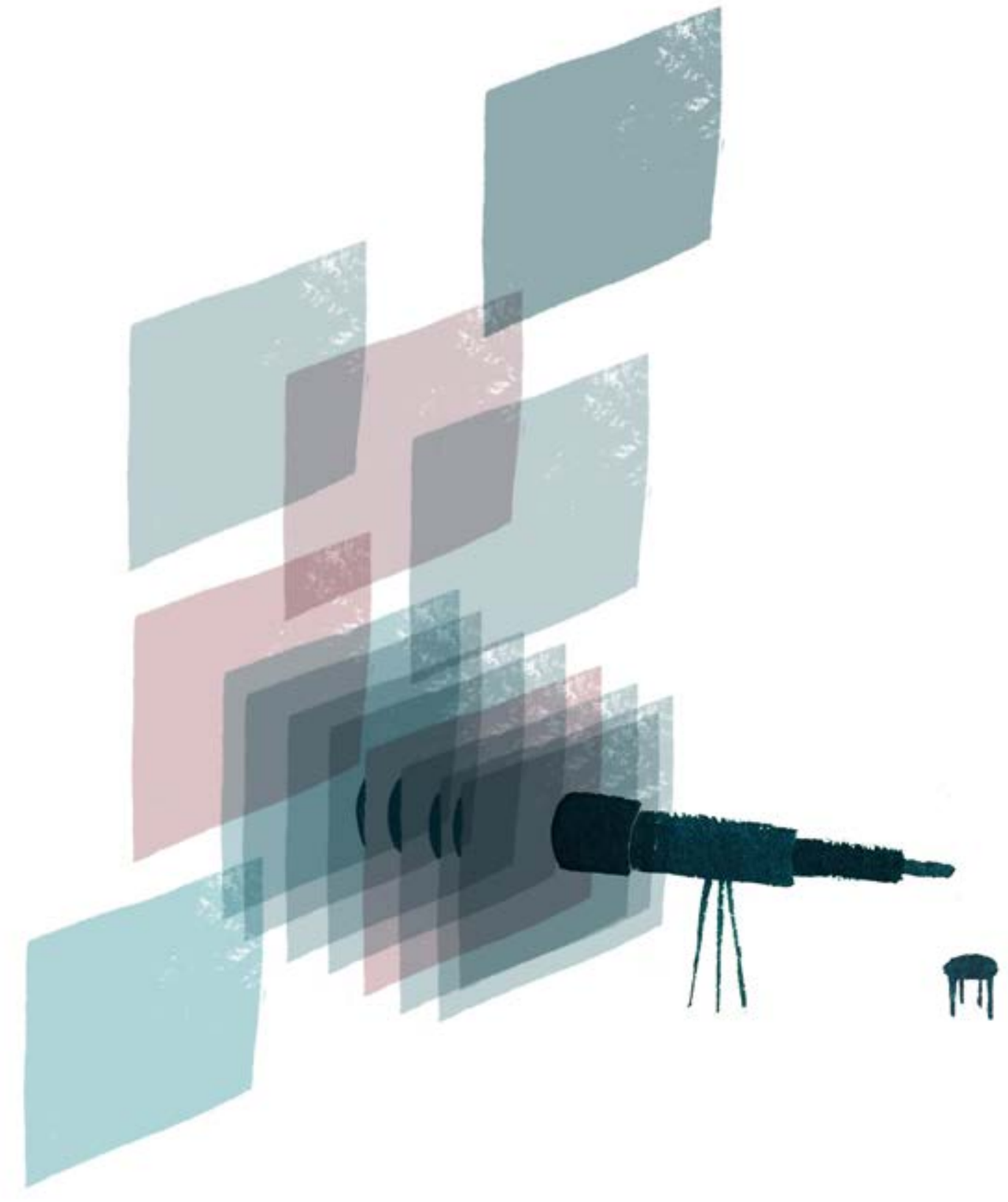
A discordância fundamental entre aqueles que argumentam que as comunicações devem ser encriptadas para proteger o conteúdo de intromissões, e aqueles que defendem que não devem ser encriptadas para que as agências estatais possam acessar o conteúdo de qualquer troca de informações tem em seu centro o dano que os governos e seus órgãos estatais provocam em escala nas populações e a consequente falta de confiança nas agências governamentais e na aplicação da lei que se desenvolveram ao longo do tempo.

É também importante reconhecer que a pressão dos Estados para restringir a criptografia foi, e continua sendo, destinada a uma série de finalidades diferentes a nível global e mudou ao longo do tempo. O foco atual da regulamentação emergente da UE está no material de abuso sexual infantil, já nos EUA o combate ao terrorismo foi uma força motriz para a reforma desde o 11 de setembro. No Brasil, o governo afirmou[17] que é essencial combater o crime, o suborno e a corrupção,[18] enquanto na Índia a violência das massas e as ligações com a desinformação são os atuais motivadores políticos.

A privacidade no ambiente digital é, sem dúvidas, um dos fatores mais importantes na forma como empoderamos e controlamos indivíduos e sociedades. As crianças de hoje podem ser a primeira geração na qual, como numa tempestade perfeita, combinam-se a existência de informações digitais onipresentes e vigilância estatal e comercial onipresentes. Esse é o contexto no qual ocorre o debate sobre a regulamentação da criptografia, bem como a análise de como fazer isso em respeito aos direitos das crianças.

17 Veja Riana Pfefferkorn regarding Operation Car Wash in this event organised by the Stanford Cyber Policy Center: https://www.youtube.com/watch?v=K0myjgC3Aho&ab_channel=FSIStanford

18 Fishman, A. et al., *The Secret History of US Involvement in Brazil's Scandal-Wracked Operation Car Wash,* 12 de março de 2020, https://theintercept.com/2020/03/12/united-states-justice-department-brazil-car-wash-lava-jato-international-treaty/



# Entendendo a criptografia e seu lugar no ambiente digital

Desenvolver uma abordagem do direito das crianças à criptografia requer um entendimento minucioso dessa tecnologia: como funciona, como é utilizada e integrada no ambiente digital. Quando se trata de decisões de se e como aplicar criptografia, elas possuem consequências em nível individual, comunitário, estatal e internacional.

Alguns reguladores perceberam que cada provedor é diferente e tem arquiteturas, modelos de negócios e bases de usuários diversos. Isso significa que uma intervenção ou uso de uma ferramenta específica em uma plataforma pode não ser proporcional em outra.[19] Por isso, é importante definir a tecnologia e explorar suas diferenças e nuances em discussões técnicas.

Muitas vezes se fala nos debates recentes em "criptografia forte" ou "quebrar criptografia" ou "burlar" a criptografia. O que isso realmente significa na linguagem do dia a dia? Por que isso importa no debate atual sobre crianças no ambiente digital?

## Criptografia e Internet

Para entender o que é criptografia e porque ela importa, devemos primeiro entender alguns aspectos básicos do funcionamento da Internet e da World Wide Web.

O guia de Beck Hogge, Internet Policy and Governance for Human Rights Defenders,[20] oferece uma explicação útil sobre a construção da Internet e como a World Wide Web funciona nela, descrita em sete camadas separadas, cada uma "empilhada" sobre a última.[21] TO modelo ajuda a dar um senso de lugar aos usuários do dia a dia, atores e *stakeholders* envolvidos em cada parte do seu design, desenvolvimento, manutenção e modelos existentes de governança.

Quase todo debate recente nos espaços anglo e eurocêntricos sobre "criptografia", "plataformas" e criança apenas considera o conteúdo, usuários e suas interações em uma camada superficial na qual o conteúdo pode ser visto. Entretanto, métodos seguros de gerenciamento de diferentes partes da Internet dependem da crip-

19 Australian eSafety Commissioner, *Basic Online Safety Expectations. Responses to transparency notices*, 2022, https://www.esafety.gov.au/industry/basic-online-safety-expectations/responses-to-transparency-notices

20 Hogge, B., *Travel Guide to the Digital World: Internet Policy and Governance for Human Rights Defenders*, 2014, https://www.gp-digital.org/wp-content/uploads/2014/06/Travel-Guide-to-the-Digital-Worlds-1.pdf

21 Ver: https://computersciencewiki.org/index.php/OSI_model

tografia em todo conjunto completo de camadas, ou na "pilha" de sua construção. Essa é a razão pela qual algumas pessoas afirmam, por exemplo, que, se você banir a criptografia online, você impede serviços bancários e comerciais seguros.

Como Hogge descreve em seu guia,[22]

> *"Operadores de rede podem censurar e monitorar conteúdo na camada física. Na camada de código, a IETF e a ICANN definem padrões e mantêm as funções-chave da Internet. A camada das aplicações é hospedeira das grandes empresas tecnológicas como Google e Facebook, cujos serviços a dominância de mercado conspirou para fazer as 'praças públicas' da era digital"*
>
> Becky Hogge, *Internet Policy and Governance for Human Rights Defenders*

## Como funciona a comunicação na World Wide Web?

De forma simples, dados são enviados através da Internet em "pacotes" de um dispositivo digital para outro, divididos em parcelas manejáveis que fluem em um fluxo de tráfego ou dados eletrônicos. Entretanto, da mesma forma que o que é enviado por meio de um serviço postal, o remetente não tem controle do que acontece com sua parcela, uma vez enviada. Existem, dessa forma, mecanismos e acordos para instruir cada parte do sistema sobre como administrar e distribuir os pacotes. Essas instruções precisam ser legíveis e compreendidas em toda World Wide Web, para que as funções e tarefas administrativas sejam codificadas em instruções amplamente acessíveis em toda a Internet. Esse tipo de padrão está sendo constantemente refinado aprimorado, e novos padrões estão sendo construídos onde necessário.

Cada pacote de informação pode ser enviado em uma variedade de formas, e pode ser enviado "às claras", de forma que qualquer pessoa com acesso ao pacote em qualquer ponto da jornada possa ver seus conteúdos - na prática, a distribuição de uma carta aberta sem um envelope.

Alternativamente, remetente e destinatário podem codificar os dados por meio de criptografia, que é comumente pensada como um método utilizado para preservar a confidencialidade entre partes que querem enviar, compartilhar e armazenar informações sem que tudo seja visível para o exterior. Nesse sentido, a criptografia é utilizada para proteger os conteúdos dos dados transmitidos. Mas também é possível proteger a ferramenta de transporte, e não apenas o que está dentro dele.

Aqui é onde o termo "metadados" importa, que é na prática a rotulação e informação descritiva adicionada à parte externa dos pacotes, incluindo endereços do remetente e destinatário, que permite a todos os pacotes chegarem no mesmo lugar e serem colocados juntos de volta na ordem correta, para que o destinatário os receba e leia como o remetente pretendeu.

Quando criptografia é utilizada "em trânsito" com a intenção de prevenir que terceiros que possam interceptar o conteúdo dos pacotes de dados sejam capazes de lê-los enquanto são movidos de um lugar para outro, e que apenas possam ser lidos pelo remetente antes de ser enviado ou depois que recebidos pelo destinatário, a isso se dá o nome de criptografia de ponta a ponta.

> *"A Internet vem sendo chamada de 'mundo de fins' e uma 'rede de ponta a ponta', porque na Internet a coisa que importa, a coisa inteligente, acontece nas pontas, nos computadores que se conectam a ela. Os computadores que se conectam à Internet estão constantemente gerando, armazenando e compartilhando informações."*
>
> Becky Hogge, *Internet Policy and Governance for Human Rights Defenders*

Uma importante ressalva deve ser lembrada quando definimos o que criptografia de ponta a ponta significa na prática. Se os servidores, enviando, armazenando e recebendo dados, controlam as chaves criptográficas - as chaves utilizadas para decodificar os dados - utilizadas nos servidores, e não nos usuários da ponta, o operador do servidor terá acesso aos dados. Portanto, o ambiente não é controlado pelas escolhas dos usuários sobre criptografia, e o controlador do servidor será capaz de acessar seu conteúdo e fornecê-lo às forças de aplicação da lei mediante solicitação.

## O que a criptografia faz por mim na World Wide Web?

A criptografia é parte fundamental da criação de websites seguros. Entretanto, recentes avanços na segurança de páginas web levou alguns a argumentarem que a criptografia de ponta a ponta é prejudicial à proteção de crianças online.

Quando usuários visitam uma página web, veem dados que são hospedados naquele website porque informação eletrônica é transferida entre onde está armazenada para o "navegador" do usuário (por exemplo, Google Chrome, Microsoft EDGE, Mozilla Firefox). Mas como um computador encontra o site que você quer entre bilhões de páginas web no mundo?

O Sistema de Nomes de Domínio ("DNS") é um sistema para nomeação e identificação de computadores alcançáveis através da Internet ou outras redes de Protocolo de Internet. É o sistema que permite humanos buscarem o endereço web e obter o que conhecemos como nomes de domínio (por exemplo, https://home.crin.org/) "resolvido" em endereços IP numéricos que o computador pode encontrar (como 198.185.159.144), e vice-versa.

22 Hogge, B., *Travel Guide to the Digital World: Internet Policy and Governance for Human Rights Defenders*, 2014, p. 46.

Esse sistema de nomeação existe para que encontrar websites seja mais fácil para as pessoas, as quais normalmente acham mais difícil memorizar uma longa cadeia de números. O DNS atua como um livro de endereços que humanos e computadores podem ambos entender.

Várias empresas de navegadores aprimoraram a segurança do usuário nos últimos anos para garantir que eles usem DNS sobre HTTPS (DoH). Isso significa que dados são criptografados quando transferidos do computador onde estão armazenados para o navegador da pessoa que está vendo o website. Websites que usam esse tipo de proteção (chamado SSL/TLS) começam com "https" ao invés de "http". Esse desenvolvimento tem o objetivo de fazer o acesso a websites mais seguro, prevenindo falsa autenticação por *"ataques man-in-the-middle"*.

Ataques *man-in-the-middle* se referem a situações nas quais um estranho interfere em dados que estão sendo transferidos, por exemplo, fingindo mostrar aos usuários o website que eles estão tentando visitar, mas modificando detalhes importantes dele. Aquele que promove o ataque pode, por exemplo, direcionar a entrada do dado de detalhes do cartão de crédito do usuário para um ponto final diferente para roubar (ou promover "phishing") informações pessoais e financeiras.

Cloudflare, um provedor de serviços de nuvem global, explica da seguinte forma:[23]

> *"SSL garante que qualquer um que intercepte os dados possa ver apenas uma bagunça de caracteres embaralhados. O número do cartão de crédito do consumidor está agora seguro, visível apenas para o website da loja onde ele o inseriu"*
>
> *"SSL também interrompe certos tipos de ciberataques: autentica servidores web, o que é importante porque atacantes vão normalmente tentar montar websites falsos para enganar usuários e roubar dados. Ele também previne atacantes de interferir em dados em trânsito, como um "lacre à prova de violação em um recipiente de medicamento".*

## Criptografia em websites e os desafios de identificar conteúdo ilegal e prejudicial

A virada para maior segurança dos websites por meio do "HTTPS sobre DNS" ou "DoH" criou desafios para algumas organizações responsáveis pela criação de listas de websites a serem bloqueados ou monitorados. Por exemplo, a Internet Watch Foundation (IWF) do Reino Unido escaneia páginas web para criar listas de websites que contêm conteúdo ilegal ou prejudicial para crianças, incluindo conteúdo relacionado a terrorismo ou pornografia. Isso possibilita o bloqueio de sites que contêm tais conteúdos e a criação de listas de páginas a serem vigiadas para que outros possam monitorar quando seus usuários estão acessando esse tipo de material.

Em fevereiro de 2020, o Firefox adotou DNS sobre HTTPS por padrão para usuários nos Estados Unidos, tornando sua experiência de navegação mais segura por padrão. De acordo com John Dunn escrevendo para Sophos,[24]

> *"Para entusiastas da privacidade, essa mudança foi boa porque não é da conta de [Provedores de Serviço de Internet], nem de governos saber quais domínios os usuários visitam. Para PSIs, por contraste, DoH traz a eles diversas dores de cabeça, incluindo como cumprir com suas obrigações legais no Reino Unido de armazenar o equivalente a um ano de visitas de cada assinante da Internet no caso de o governo querer investigá-los futuramente para evidências de atividades criminais"*

O Reino Unido já é reconhecido por ter uma das abordagens mais intrusivas de demandas estatais para os provedores de serviços de Internet. Empresas que querem promover uma arquitetura web mais segura, "HTTPS sobre DNS", incluem provedores de DNS que oferecem mecanismos de filtragem e controle parental. Entretanto, a Internet Service Providers Association (ISPA)[25]— uma associação comercial que representa PSIs britânicos - e a British Internet Watch Foundation criticaram a Mozilla, organização sem fins lucrativos responsável pelo navegador Firefox, por apoiar DoH, dizendo que irá enfraquecer programas de bloqueio web, incluindo a filtragem PSI por padrão de conteúdo adulto e a filtragem obrigatória ordenada por violação de direitos autorais, as quais dependem de arquiteturas menos seguras para serem efetivas. A Mozilla respondeu colocando que DoH não será utilizado por padrão no mercado britânico até haver mais discussões com *stakeholders* relevantes, mas enfatizou que, se fosse implementado, "ofereceria benefícios de segurança reais aos cidadãos do Reino Unido".[26]

Na realidade, essa solução alternativa é explorada por algumas empresas, por exemplo, aquelas que vendem sistemas e serviços de filtragem web (e monitoramento de usuários) a atores de educação. Eles se colocam como se fossem um site real, mas, na verdade, são imitações.

Filtrar conteúdos significa ter acesso a eles primeiro. De acordo com Professor Ross Anderson, filtros, essencialmente, são um entre três tipos existentes, dependendo de em qual nível operam.[27] Filtragem de pacotes, gateways de circui-

23 Veja: https://www.cloudflare.com/en-gb/learning/ssl/what-is-ssl/

24 Dunn, J., *ISPs call Mozilla 'Internet Villain' for promoting DNS privacy*, 2019, https://nakedsecurity.sophos.com/2019/07/08/isps-call-mozilla-internet-villain-for-promoting-dns-privacy/

25 ISPA, *ISPA withdraws Mozilla Internet Villain Nomination*, 2019, https://www.ispa.org.uk/ispa-withdraws-mozilla-internet-villain-nomination-and-category/

26 The Guardian, Firefox: 'no UK plans' to make encrypted browser tool its default, 2019, https://www.theguardian.com/technology/2019/sep/24/firefox-no-uk-plans-to-make-encrypted-browser-tool-its-default

27 Anderson R., *Security Engineering—A Guide to Building Dependable Distributed Systems*, 2020, Chapter 21, https://www.cl.cam.ac.uk/~rja14/book.html

to (onde filtragem de DNS acontece) e aplicações proxies (filtros de e-mail que tentam eliminar spam). Desde a adoção de rotas de transportes mais seguras via HTTPS, as ferramentas para realizar tais trabalhos foram deslocadas para as pontas dos sistemas e redes.

A criptografia sozinha não protege confidencialidade, prática comercial ou conteúdo das comunicações. Apenas protege contra observadores terceiros indesejados. Não garante o que indivíduos ou instituições - as "pontas" - fazem depois disso, com os (agora desencriptados) dados.

Isso é especialmente importante para lembrar quando se estar considerando se um método de criptografia é mais "preservador da privacidade" que outro, ou quando avaliando se uma intervenção tecnológica particular em um ponto do processo "interfere" ou não com a privacidade. Criptografia não é uma única ferramenta em um único ponto de um processo físico, mas múltiplos tipos podem estar envolvidas em qualquer tipo de comunicação online. O princípio e prática em jogo é se há alguma interferência de terceiros.

Por que esse entendimento importa? Porque criptografia é necessária para manter usuários seguros e discussões que colocam "criptografia" como a única ameaça faz com que encontrar soluções viáveis para endereçar os problemas reais sejam mais difíceis. Como descrito por Dr. Ian Levy e Crispin Robinson do GCHQ em 2018 em um artigo no Lawfare[28]:

> *"Coletivamente, nos definimos os vários problemas de serviços e dispositivos como uma única entidade chamada 'criptografia'. Isso não é útil, pois limita detalhes de cada dispositivo e serviços e impulsiona soluções específicas"*

## Criptografia e metadados

Metadados é informação sobre outros dados. Na conversa sobre comunicação digital, metadados podem incluir informações sobre a origem dos dados, sua estrutura, armazenamento e como é armazenado. Por exemplo, se um dado é originado de celular, os metadados podem incluir nome, *firmware*, tipo de dispositivo, configuração e capacidade desse celular.

Metadados normalmente incluem informações úteis para os provedores de serviços utilizados nos processos de comunicação, tais quais como bem está o desempenho, quão rápido informações estão sendo escritas e lidas e quão rápidos sistemas estão respondendo. Por exemplo, se a informação que está sendo transmitida inclui áudio ou vídeo, é importante para os provedores de serviços otimizarem a velocidade e ordem como os pacotes de dados estão sendo enviados, recebidos e reconstruídos para melhorar a experiência dos usuários. Metadados também incluem informações sobre servidores, computadores e outros dispositivos de onde o dado veio, foi e é armazenado.

28 Levy, I. and Robinson, C., *Principles for a More Informed Exceptional Access Debate*, 2018.



Criptografia que protege os conteúdos das comunicações não protege os metadados no qual o remetente e destinatário não criaram, mas as quais sem elas os pacotes não podem passar pelas diferentes partes do sistema, porque o roteamento da informação precisa ser legível para que a mensagem chegue aos destinatários corretos.

No WhatsApp, conteúdo e metadados são ambos criptografados,[29] o que significa que sistemas de inteligência artificial não podem escanear todas as mensagens, imagens e vídeos automaticamente como eles fazem no Facebook e Instagram. Entretanto, os metadados ainda são visíveis pela empresa controlada pela Meta, de forma que eles possam direcionar as mensagens para o usuário correto. Ela também pode acessar informação dos conteúdos se os usuários fizerem backup de suas mensagens e interagir com uma conta *business* na plataforma.[30] Revisores de moderação de conteúdo podem ganhar acesso às comunicações quando usuários clicam no botão "denunciar" no aplicativo, e indicam que a mensagem está violando os termos de serviços da plataforma, incluindo sextorsão, desde 2020.[31]

Metadados são planejados para serem lidos por máquinas, mas como metadados são muito detalhados, também podem ser utilizados para informar muito sobre relações e comportamentos das partes envolvidas em qualquer atividade de comunicação digital, mesmo sem ver o que está contido no conteúdo.

Quando empresas de publicação digital adiciona metadados em artigos acadêmicos ou materiais educacionais para catalogar atributos dos conteúdos da biblioteca, eles são usados, por exemplo, por ferramentas de busca automatizada para identificar, perfilar e encontrar materiais que preenchem o critério de busca de todos em bilhões de conteúdos de pesquisa de páginas de Internet. De formas similares, metadados sobre comunicações podem ser utilizados para identificar, perfilar e encontrar indivíduos conversando entre si dentre bilhões de pessoas *online* no mundo.

29 WhatsApp Encryption Overview Version 6 Updated November 15, 2021. Comunicação entre clientes do WhatsApp e servidores das mensagens é separadas em canais de camadas criptografadas utilizando Noise Pipes com Curve25519, AES-GCM e SHA256 do Noise Protocol Framework. https://web.archive.org/web/20221130062942/https://scontent-lcy1-1.xx.fbcdn.net/v/t39.8562-6/309473131_1302549333851760_6207638168445881915_n.pdf?_nc_cat=107&ccb=1-7&_nc_sid=ad8a9d&_nc_ohc=kqXq2gkRQegAX_fbxBa&_nc_ht=scontent-lcy1-1.xx&oh=00_AfDWug1Zxaocf-mudtpA4Y7fhIifJV3WcpTK4H8C6Tl4kA&oe=638BB35D; See Mooney, N., *An Introduction to the Noise Protocol Framework*, 2020, https://duo.com/labs/tech-notes/noise-protocol-framework-intro

30 Cloud API, operada pela Meta, atua como um intermediário entre WhatsApp e a Cloud API businesses. Em outras palavras, aquelas empresas que deu à Cloud API o poder de operar em seu nome. Por causa disso, WhatsApp passa todo trafego de mensagens destinadas para essas empresas para a Cloud API. WhatsApp também espera receber todo do Cloud API todo trafego de mensagens dessas empresas: https://developers.facebook.com/docs/whatsapp/cloud-api/overview/data-privacy-and-security

31 ProPublica, *How Facebook Undermines Privacy Protections for Its 2 Billion WhatsApp Users*, 2021, https://www.propublica.org/article/how-facebook-undermines-privacy-protections-for-its-2-billion-whatsapp-users

David Cole, diretor jurídico nacional da ACLU e o Honorário George J. Mitchell, Professor em Direito e Política Pública no Centro de Direito da Universidade de Georgetown, memoravelmente citaram o Conselheiro Geral da NSA em um debate em 2014, dizendo que "metadados contam absolutamente tudo sobre a vida de alguém. Se você tem metadados suficientes, você não precisa do conteúdo", para explicar como metadados sozinhos podem fornecer uma imagem extremamente detalhada das associações e interesses mais íntimos de uma pessoa. É muito mais fácil enquanto tarefa tecnológica pesquisar uma grande quantidades de metadados do que escutar milhões de chamadas telefônicas. Seu co-painelista no debate, General Michael Hayden, ex-diretor da NSA e da CIA, chamou o comentário de Baker de "absolutamente correto" e adicionou, "Nós matamos pessoas com base em metadados".[32]

O Alto Comissariado para os Direitos Humanos da ONU descreveu em 2018 porque a questão de confidencialidade se aplica tanto para o conteúdo das comunicações, como para metadados: "A proteção do direito à privacidade é amplo, estendendo-se não apenas para a quantidade substantiva de informações contidas nas comunicações, mas igualmente para metadados, pois, quando analisados e agregados, tais dados podem dar insights sobre o comportamento de indivíduos, suas relações sociais, preferências privadas e identidade que vão além do que é transmitido acessando o conteúdo de sua comunicação."[33]

## Utilizando metadados para identificar abuso e exploração sexual infantil online

A potência dos metadados é uma das razões pelas quais tecnólogos argumentam que não é necessário ou proporcional acessar o conteúdo das comunicações de todas as pessoas por meio de vigilância em massa, já que metadados podem indicar padrões de comportamento que oferecem grande quantidade de informações sobre atividades ilegais. Algumas pessoas argumentam que metadados deveriam ser utilizados para identificar e justificar quando e onde intervenções direcionadas poderiam ser feitas para acessar comunicações, baseadas em suspeita, ao contrário de vigilância ou interceptação em massa, sujeitas à supervisão judicial.

O processo também funciona de forma reversa. De acordo com Dr. Ian Levy e Crispin Robinson, do GCHQ, em todos os casos, uma vez que uma imagem é classificada como abuso sexual infantil, o provedor de serviço sabe por meio dos metadados do serviço as identidades das contas que compartilharam tal conteúdo, aquelas que o receberam e aquelas que o recompartilharam. Conhecer essas informações quer dizer que mensagens educacionais poderiam ser direcionadas aos usuários relevantes e, se necessário, mandados de busca poderiam ser expedidos em face dos usuários que cometam esse tipo de infração.[34] O poder dos potenciais usos de metadados levou alguns autores engajados em reformas regulatórias do ambiente online a sugerirem que a adoção de esforços razoáveis para identificar material de abuso sexual infantil fosse considerada um princípio de nível superior:

> *"Toda plataforma compreende diferentes formas de metadados, coletando-os, avaliando-os de maneiras particulares. Os metadados apenas podem sugerir que algo é ilegal ou danoso, nunca podem dizê-lo com certeza [...] Tudo o que podem dizer é que existem fatores que indicam que pode haver algo de ilegal e danoso e, a partir disso, deve ser realizada a revisão humana. Esses fatores e pesos que eles têm variam imensamente de plataforma para plataforma. Por isso é tão difícil regular ao nível de toda a indústria, e não estou certo se é necessário que exista uma regulação específica em relação ao uso de metadados [...] [Entretanto, poderia] exigir-se de plataformas que adotem esforços razoáveis para identificar [material de abuso sexual infantil], e assim o regulador pode avaliar se as empresas estão fazendo isso, se estão utilizando os metadados que coletam da forma mais efetiva possível, e requisitar a elas que para tomem medidas adicionais caso não o estejam fazendo."*[35]

> *"São uma ferramenta muito poderosa, os metadados, e potencialmente muito intrusiva. Nós definitivamente somos fortemente contra a coleta ou escaneamento massivos de metadados. Metadados deveriam ser utilizados de forma muito específica, o que significa que outras técnicas precisariam ser utilizadas primeiro para identificar os suspeitos. Essa não é, eu acho, a forma como muitas pessoas veem metadados resolvendo esse problema, porque elas querem utilizá-los de forma massiva, para realização de grandes análises e correspondência de padrões para tentar encontrar indivíduos potencialmente suspeitos"*[36]

> *Muitos metadados são gerados [...] Eu acho que é uma de uma gama de abordagens que empresas deveriam estar trabalhando em aprimorar [...] Mesmo que ainda deixe brechas significativas, eu acho que é importante ter um processo com governos para pensar sobre como empresas podem usá-los de forma mais efetiva sem comprometer os direitos das pessoas"*[37]

32 Cole, D., '*We Kill People Based on Metadata*', 2014, https://www.nybooks.com/online/2014/05/10/we-kill-people-based-metadata/. O comentário completo pode ser ouvido em contexto no debate em: https://www.youtube.com/watch?v=kV2HDM86XgI.

33 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/39/29, 3 August 2018, para. 6, https://www.ohchr.org/en/documents/reports/ahrc3929-right-privacy-digital-age-report-united-nations-high-commissioner-human

34 Levy, I. and Robinson, C., *Thoughts on child safety on commodity platforms*, 2022, p. 64, https://arxiv.org/pdf/2207.09506.pdf

35 CRIN and ddm entrevista com Richard Wingfield, 6 September 2022.

36 CRIN and ddm entrevista com Privacy International, 26 September 2022.

37 CRIN and ddm entrevista com Ian Brown, 6 October 2022.

## Uso de criptografia para além da confidencialidade

A criptografia tem valor e usos que vão além de proteger informações confidenciais. A importância de entender como aplicações criptográficas vão além de manter as coisas confidenciais é vital na análise de riscos e benefícios, de acordo com o advogado britânico Neil Brown:

> *"Se você focar apenas em uma solução como 'boa suficiente' para confidencialidade e ignorar as outras facetas da criptografia, sua solução provavelmente será inadequada"*[38]

Ele identificou doze áreas nas quais a criptografia tem um papel, além da confidencialidade, incluindo:

- **Anonimato:** mantém desconhecida a identidade de alguém para outra pessoa ou grupo de pessoas, ou para um ou mais provedores de serviços;
- **Assincronicidade:** a habilidade de alguém enviar uma mensagem, mesmo se o destinatário está *offline*, ou enviar para alguém que irá receber uma mensagem, mesmo se o remetente da mensagem está *offline*; e
- **Autenticação:** verificar que a informação criptografada foi encriptada corretamente, utilizando o algoritmo de encriptação escolhido.

Mais importante, "criptografia" não é uma tecnologia única ou uma coleção de diferentes ferramentas. Brown descreve "criptografia" como um conceito, ou um conjunto de processos em um sistema. Na prática, o processo de encriptação é realizado por meio de algoritmos e nem todos os algoritmos são iguais, ou tentam fazer as mesmas coisas. Alguns algoritmos têm diferentes capacidades e são melhores para algumas tarefas do que outras. Alguns algoritmos demandam mais dos usuários que outros - por exemplo, mais recursos computacionais ou mais habilidades técnicas para serem aplicados.[39]

## Criptografia na vida do dia a dia de crianças

Crianças se beneficiam do uso de criptografia que é aplicada em seu dia a dia, em cibersegurança e privacidade, assim como os adultos. Um fio condutor entre as esferas da privacidade e da segurança infantil é a questão da interferência. Quem pode interferir em uma criança, em seu livre e completo desenvolvimento, suas atividades e comunicações diárias? Como? Com qual efeito? E com quais propósitos?

Os domínios nos quais a segurança pode proteger crianças e mantê-las seguras, onde elas estão ativamente online, incluem não só comunicações e redes sociais, mas o acesso a finanças, saúde, educação, política, participação na cultura e na comunidade, e jogos. Nesses ambientes, tecnologias inseguras já afetaram crianças significativamente.

Em 2011, foi relatado que dados de 77 milhões de usuários da Sony PlayStation haviam sido roubados. "Pessoa ilegal e não autorizada" obteve nomes, endereços, endereços de e-mail, datas de nascimento, nomes de usuário, senhas, logins, perguntas de segurança. E mais, a Sony relatou que crianças com contas criadas por seus pais também podem ter tido seus dados expostos.[40]

Em 2015, a empresa de tecnologia e brinquedos infantis Vtech suspendeu as negociações na bolsa de valores de Hong Kong após admitir ter sofrido uma invasão que supostamente resultou no roubo de 5 milhões de dados, incluindo informações sensíveis e registros não encriptados de bate-papo entre crianças e seus pais.[41]

Em 2016, o *Norwegian Consumer Council* [Conselho de Consumidores da Noruega] (NCC) identificou problemas em brinquedos conectados à Internet que são emblemáticos no crescimento da disseminação de dispositivos conectados. O NCC afirmou que, em um mercado em expansão, é essencial que consumidores, especialmente crianças, não sejam utilizados como cobaias para produtos que não foram suficientemente testados.[42]

Em 2017, em parceria com a empresa de segurança *Mnemonic,* o NCC também testou diversos dispositivos de *smartwatch* para crianças. Os pesquisadores descobriram falhas de seguranças significativas, recursos de seguranças não confiáveis e falta de proteção aos consumidores. Finn Myrstad, Diretor de Política Digital do NCC, afirmou no momento que:

> *"É bastante sério quando produtos que afirmam deixar crianças mais seguras, na realidade, colocam-nas em risco devido a pouca segurança e recursos que não funcionam corretamente."*[43]

Na área da educação, o *Federal Bureau of Investigation* [Departamento Federal de Investigação] dos Estados Unidos (FBI), a *Cybersecurity and Infrastructure Security Agency* [Agência de Cibersegurança e Segurança em Infraestrutura] (CISA), e o *Multi-State Information Sharing e Analysis Center* [Centro Multiestadual

38 Brown, N., *The end to end encryption debate: 1: the (very) basics of "encryption"*, 2022, https://neilzone.co.uk/2022/01/the-end-to-end-encryption-debate-1-the-very-basics-of-encryption

39 Para mais informação na dimensão de conceitos técnicos e legais envolvendo criptografia, veja: UK Information Commissioner's Office, *What is Encryption?*, 2022, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/encryption/what-is-encryption/

40 Reuters, *Sony PlayStation suffers massive data breach*, 27 April 2011, https://www.reuters.com/article/us-sony-stoldendata-idUSTRE73P6WB20110427

41 VICE, *One of the Largest Hacks Yet Exposes Data on Hundreds of Thousands of Kids*, 27 November 2015, https://www.vice.com/en/article/yp3z5v/one-of-the-largest-hacks-yet-exposes-data-on-hundreds-of-thousands-of-kids. The breach of the popular kids' gadgets company VTech also exposed children's pictures and recordings, and chats with their parents: VICE, *Hacker Obtained Children's Headshots and Chatlogs From Toymaker VTech*, 30 November 2015, https://www.vice.com/en/article/yp3zev/hacker-obtained-childrens-headshots-and-chatlogs-from-toymaker-vtech

42 See: https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/

43 Ver: https://www.forbrukerradet.no/side/significant-security-flaws-in-smartwatches-for-children/

de Compartilhamento de Informações e Análises] (MS-ISAC) reconheceram em 2022 que ambientes educacionais são de alto risco para ataques de *ransomware*, uma vez que capacidades limitadas de cibersegurança e recursos limitados aumentam sua vulnerabilidade e "instituições K-12[44] são vistas como alvos lucrativos pela quantidade de dados sensíveis de estudantes acessíveis por meio do sistema das escolas ou administradas por provedores de serviços".[45]

No ambiente familiar, uma criança pode experienciar um conflito entre sua própria agência e os direitos e responsabilidades de seus pais, particularmente em lares culturalmente conservadores. Essas considerações são relevantes quando consideramos serviços de monitoramento ou controle parental nos celulares, ou outros dispositivos de crianças. Para oferecer vigilância parental ou serviços de monitoramento nos dispositivos móveis das crianças, *apps* de controle parental requerem acesso privilegiado aos recursos dos sistemas e acesso a dados sensíveis.

De acordo com Fael, "isso pode implicar na redução dos perigos associados às atividades online das crianças, mas levanta preocupações significativas em relação à privacidade. Essas preocupações têm sido até agora negligenciadas por organizações que fornecem recomendações de uso de aplicações de controle parental ao público."[46]

Em uma avaliação de 2021 que cobriu 3.264 aplicativos de controle parental , os pesquisadores Wang et al. concluíram que eles estavam sendo cada vez mais adotados por pais como forma de proteção da segurança *online* de seus filhos.[47] Entretanto, não estava claro se esses aplicativos eram sempre benéficos ou efetivos no cumprimento de seus objetivos; por exemplo, o uso excessivo de restrições e vigilância prejudicou a relação entre pais e filhos e o senso de autonomia das crianças. Ghosh et al. identificaram em 2018 que, de forma geral, o aumento de controle parental estava associado a mais (e não menos) riscos online.[48]

44 N.T: Abreviatura referente ao sistema de ensino dos Estados Unidos. Designa o período referente ao jardim da infância (Kindergarten) até o 12º grau (High School Senior)

45 US Cybersecurity and Infrastructure Security Agency, *Alert (AA22-249A) #StopRansomware: Vice Society*, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-249a.

46 Feal, Á. et al., *Angel or Devil? A Privacy Study of Mobile Parental Control Apps*, 2020, Proceedings on Privacy Enhancing Technologies 2020 (2): 314 - 335, https://petsymposium.org/popets/2020/popets-2020-0029.php

47 Wang, G. et al., *Protection or punishment? Relating the design space of parental control apps and perceptions about them to support parenting for online safety*, 2021, Proceedings of the Conference on Computer Supported Cooperative Work Conference, 5(CSCW2), https://ora.ox.ac.uk/objects/uuid:da71019d-157c-47de-a310-7e0340599e22

48 Ghosh, A. et al., *A Matter of Control or Safety?: Examining Parental Use of Technical Monitoring Apps on Teens' Mobile Devices*, 2018, Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, https://www.semanticscholar.org/paper/A-Matter-of-Control-or-Safety%3A-Examining-Parental-Ghosh-Badillo-Urquiola/67ed9c02529ecfba7fe35cf8ec1bfdc42dbc73c8



Dr. Ian Levy e Crispin Robinson também apontam em seu artigo recém-publicado:

> *"Esse tipo de mecanismo pode colocar algumas crianças em risco adicional em relação a pais abusivos ou manipuladores, mesmo quando eles não têm acesso a conteúdo, e, embora a técnica seja relativamente simples em escala, pesquisas seriam necessárias para determinar quão bem poderia abranger usuários em maior risco e como crianças em risco poderiam estar efetivamente protegidas."*

Segurança é um processo, não um produto. A criptografia pode transformar a confiança em um código legível por máquina para que máquinas possam verificar e confiar umas nas outras, mas a confiança humana ainda depende dos indivíduos, uns em relação aos outros. Usar ferramentas para substituí-la traz consequências.

## Escaneando conteúdo descriptografado para encontrar imagens conhecidas

Desenvolvimentos tecnológicos permitiram novas rotas para acessar e abusar de crianças, tanto em tempo real, como por meio de distribuição repetida de conteúdo e, em resposta, novas tecnologias estão sendo desenvolvidas e aplicadas para responder a esses desafios.

Quando se trata de detecção e moderação de conteúdo, para identificar e remover imagens de abuso sexual infantil, a tecnologia mais conhecida é o *PhotoDNA*, criado pelo professor Hany Farid e adquirido pela *Microsoft*.

*O PhotoDNA*[49] funciona criando uma assinatura digital única (conhecida como "hash") de uma imagem, que é comparada com hashes de outras imagens para encontrar cópias da mesma imagem. Isso se desenvolve em um ambiente não criptografado. O Facebook adota o PhotoDNA desde 2010 em toda sua rede, o *Twitter* desde 2011 e o *Google* a partir de 2016.[50] O *software* opera em ambientes não criptografados, como a rede aberta sem HTTPS, canais sem criptografia de ponta a ponta ou em pontos onde o conteúdo armazenado não é criptografado (como no nível dos provedores de serviço de Internet).

Em 2018, ao implementar o *PhotoDNA* e para evitar a complexidade de classificar conteúdo cuja legalidade poderia ser disputada, a política do *Facebook* era apenas de "adicionar conteúdo ao banco de dados que continham imagens de crianças com menos de 12 anos envolvidas em ato sexual explicito".[51] Em 2019, *Facebook* mudou para um algoritmo diferente de *hashing*, PDQ, desenvolvido por eles mesmos e com uma versão também irá *hashear* vídeos. [52]

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

50 Farid, H., Reining in Online Abuses, 2018, Technology & Innovation, 19(3) 593–599.

51 Ibidem.

52 Meta, *Open-Sourcing Photo- and Video-Matching Technology to Make the Internet Safer*, 1 de agosto de 2019, https://about.fb.com/news/2019/08/open-source-photo-video-matching/

A crítica mais comum ao *PhotoDNA* é que ele apenas identifica imagens conhecidas. O *PhotoDNA* não é capaz de detectar imagens que não foram denunciadas ou novas imagens. Apesar disso, o antigo presidente e CEO do *National Center for Missing and Exploited Children* [Centro Nacional para Crianças Desaparecidas e Exploradas], Ernie Allen, afirma que essa é uma importante ferramenta para remoção de conteúdo para reduzir a vitimização, que pode identificar fotos em circulação há vários anos ou então que são novas mas apenas foram identificadas e transformadas em *hash* recentemente. "Utilizando o *PhotoDNA*, nós somos capazes de comparar essas imagens, trabalhando com provedores de serviços *online* ao redor do país, para podermos parar a redistribuição de tais fotos."[53]

Professor Farid também construiu uma versão modificada do *PhotoDNA*, chamada *eGlyph*, para identificação de material com propósitos de contraterrorismo. Vale destacar seus comentários feitos em um artigo de 2018, segundo os quais a aplicação direcionada a qualquer tipo de imagem não é limitada por salvaguardas construídas na tecnologia, mas sim por leis:

> *"Qualquer tecnologia como a que desenvolvemos e implementamos pode ser mal utilizada. A tecnologia subjacente é agnóstica no que busca e remove. Na implementação do PhotoDNA e do eGlyph, fomos excessivamente cuidadosos para controlar sua distribuição via disposições de licenciamento rigorosas. É minha esperança e expectativa que essa tecnologia não seja utilizada para interferir em uma Internet aberta e livre, mas sim para eliminar alguns dos piores e mais hediondos conteúdos online."*

Há uma preocupação generalizada entre especialistas em privacidade de que salvaguardas legais fornecem proteções insuficientes contra o crescente escopo para o uso da tecnologia, que vai para além da identificação de imagens de abuso sexual infantil.

> *"Muito do trabalho voluntário na detecção de CSAM é baseado nesses bancos de dados, e acontece de forma relativamente limitada. Entretanto, a tecnologia que está sendo implementada para fazer isso já está sendo aplicada para também buscar por conteúdos terroristas. Também está sendo potencialmente utilizada para procurar por desinformação."*[54]

Existe menos informação no domínio público sobre essa tecnologia que opera ao vivo e em tempo real em ambientes digitais. Um relatório independente de especialistas do Conselho Europeu de 2021[55] declarou que a Microsoft vem utilizando ferramentas com propósitos de detectar aliciamento online (grooming) baseadas em inteligência artificial (IA) e destinadas a direcionar comportamentos em programas na plataforma Xbox há anos, e estava explorando seu uso em serviços de chat, incluindo Skype. Entretanto, isso agora pode estar ultrapassado[56], pois como seus termos e condições no momento da escrita afirmam[57], "nós não monitoramos os serviços e não tentamos fazê-lo".

A esperança de algumas pessoas com quem conversamos e que apoiam vítimas e sobreviventes, são tecnologias emergentes futuras que garantam acesso em tempo real a conversas e comportamentos para um escopo mais amplo de pessoas, como profissionais de proteção, incluindo, por exemplo, o projeto do Reino Unido DRAGON-S, (Developing Resistance Against Grooming Online-Spot and Shield) [Desenvolvendo Resistência contra Aliciamento Online - Identificação e Escudo]. A proposta de fazer triagem de conversas que operadores humanos acreditam que deveriam ser inspecionadas em maiores detalhes ainda precisará respeitar princípios de direitos humanos como necessidade e proporcionalidade.[58]

Uma área de risco e dano que merece atenção no contexto mais amplo do sistema proteção de crianças é a identificação de imagens íntimas compartilhadas consensualmente entre pares, comumente conhecida como *"sexting"*. Esse ato por parte de crianças constitui ofensa criminal no Reino Unido e em muitas outras jurisdições, mas a intenção da maioria dos adultos que oferecem suporte a jovens é não criminalizá-los, e sanções formais contra eles seriam consideradas excepcionais.[59]

## Soluções alternativas à criptografia e exploração de falhas de segurança no contexto da proteção de crianças

As dificuldades na identificação de comportamento ilegal em ambientes com criptografia de ponta a ponta, incluindo exploração e abuso sexual infantil, levou a diversas propostas para superar esse desafio.

### Varredura pelo lado do cliente

Varredura pelo lado do cliente é uma forma de monitorar o conteúdo e dados de comportamento gerados em um dispositivo, em oposição a em trânsito. Isso significa que a comunicação que sai do dispositivo é escaneada e checada contra uma lista de imagens e palavras conhecidas antes de ser enviada. Se há correspon-

53 Veja: https://news.microsoft.com/2009/12/15/new-technology-fights-child-porn-by-tracking-its-photodna/

54 Entrevista de CRIN e ddm com Privacy International, 26 de setembro de 2022

55 Council of Europe, *Independent Experts' Report: Respecting human rights and the rule of law when using automated technology to detect online child sexual exploitation and abuse*, 2021, p. 24, https://rm.coe.int/respecting-human-rights-and-the-rule-of-law-when-using-automated-techn/1680a2f5ee

56 Ver: https://blogs.microsoft.com/on-the-issues/2020/01/09/artemis-online-grooming-detection/

57 See Microsoft Services Agreement from August 2022: https://web.archive.org/web/20221204112549/https://www.microsoft.com/en-gb/servicesagreement

58 This platform has been collaboratively developed with Legal Innovation Lab Wales, supported by the European Regional Development Fund through the Welsh Government: https://www.swansea.ac.uk/project-dragon-s/

59 See CRIN, *Discrimination and Disenfranchisement: A global report on status offences*, 2016, pp. 38-41, https://archive.crin.org/sites/default/files/crin_status_offences_global_report_0.pdf; See also: https://childlawadvice.org.uk/information-pages/sexting/

dência, o sistema se recusa a enviar a mensagem ou pode reportá-la para as forças policiais ou organizações de fiscalização. A varredura pelo lado do cliente vem sendo proposta como forma de identificação de material de abuso sexual infantil compartilhado em canais criptografados, escaneando as mensagens antes delas serem criptografadas e enviadas, mas não há nada sobre a técnica ou tecnologia que a limite a identificar um tipo particular de imagem ou conteúdo.

Existem também medidas de escaneamento "híbridas" similares, tais como as propostas pela Apple em 2021. Diante de críticas, a empresa decidiu mudar alguns de seus planos e pausar outros[60], mas as propostas eram para que quando usuários realizassem o *upload* de fotos nos servidores *Apple*, isso iniciasse um processo de escaneamento. Esse método de detecção de material de abuso sexual infantil não é estritamente do "lado do cliente" mas um "híbrido no dispositivo/canal do servidor". Embora a primeira fase do processo de correspondência de *hash*[61] aconteça no dispositivo, seu resultado é apenas interpretado na segunda fase, executada nos servidores de fotos do *iCloud da Apple.* A Apple anunciou uma mudança nos seus planos em dezembro de 2022 para focar seus esforços no desenvolvimento da função *Communication Safety* [Segurança de Comunicação].[62]

O plano inicial era de que, se imagens já conhecidas de abuso sexual infantil fossem upadas nos servidores de iCloud da *Apple* em um número que excedesse o limiar de revisão, a Apple iria detectar uma correspondência na base de dados de *hashes* de imagens fornecida pelo *National Center for Missing and Exploited Children.* Apesar de o sistema utilizar aprendizado de máquina para detectar alterações mínimas, como imagens cortadas ou comprimidas de maneira diferente, não seria capaz de detectar uma imagem desconhecida.

Diversos especialistas entrevistados durante a pesquisa para este relatório viram vantagens no uso de varredura pelo lado do cliente como um meio menos intrusivo em identificar o conteúdo transferido por meio de canais criptografados, já que a tecnologia não busca ter acesso a toda comunicação do usuário, mas opera antes da encriptação e depois da desencriptação da comunicação, e não "lê" as mensagens:

> *"Um mito é a ideia de olhar uma imagem ou escanear suas fotos. Isso não é o que acontece [...] Elas são 0 ou 1. Ninguém está olhando nada. Será apenas um conjunto de números comparado a outro conjunto de números. Se eles forem iguais, toma-se medidas."*[63]

60 EFF, *Apple Has Listened And Will Retract Some Harmful Phone-Scanning*, 12 de novembro de 2021, https://www.eff.org/deeplinks/2021/11/apple-has-listened-and-will-retract-some-harmful-phone-scanning

61 Apple, *Security Threat Model Review of Apple's Child Safety Features*, agosto de 2021, https://www.apple.com/child-safety/pdf/Security_Threat_Model_Review_of_Apple_Child_Safety_Features.pdf

62 CNN Business, *Apple abandons controversial plan to check iOS devices and iCloud photos for child abuse imagery*, 8 de dezembro de 2022, https://edition.cnn.com/2022/12/08/tech/apple-csam-tool/index.html

63 Entrevista de CRIN e ddm com IWF, 3 de novembro de 2022.



Entretanto, muitas pessoas e organizações que trabalham com tecnologia estão preocupadas com as propostas que apoiam a varredura pelo lado do cliente porque qualquer acesso dado a pessoas que não eram para ser parte de uma comunicação em particular precisa de uma porta de entrada. Qualquer "acesso *backdoor* aumenta a 'superfície de ataque' para comunicações criptografadas, criando formas adicionais de interferência em comunicações por meio da manipulação do banco de dados de conteúdos proibidos", e não há garantia de que será acessado apenas pelos "mocinhos", de acordo com a *Internet Society* em sua resposta ao documento de trabalho vazado de 2020 da Comissão Europeia.[64]

Quatorze especialistas em ciência da computação, vindos da Universidade de Cambridge, do Royal Society do MIT, além de um *fellow* da IEEE e dos autores do artigo *Bugs in our Pockets: The Risks of Client-Side Scanning* [Escutas em nossos bolsos: os riscos da varredura pelo lado do cliente] (2021), permanecem não convencidos e acreditam que a promessa da varredura pelo lado do cliente é uma ilusão.

Eles explicam que "mover a capacidade de escanear do servidor para o cliente abre novos pontos de vantagens para os adversários" e argumentam que se práticas e tecnologias de varredura pelo lado do cliente se tornassem generalizadas, haveria "um enorme incentivo para Estados-nações subverterem organizações que realizam a curadoria da lista de alvos, especialmente se essa lista fosse secreta".

Há críticas similares de que a varredura pelo lado do cliente, se não na prática, quebra a criptografia de ponta a ponta em princípio ao criar uma rota para interferência de terceiros, pois "fundamentalmente está muito direcionada a encontrar o conteúdo de uma comunicação criptografada de ponta a ponta: entendendo o que está para ser enviado, ou que foi enviado ou recebido em um dispositivo. Há então uma quebra da expectativa de que isso seja uma comunicação privada apenas entre seus participantes conhecidos. E, de forma mais ampla, é provável que seja incrivelmente desproporcional, devido a sua habilidade de escanear todos os tipos de conteúdos e potencialmente censurá-lo fortemente - e não apenas indicar que certo conteúdo está para ser enviado ou que foi enviado, mas potencialmente até bloquear seu envio."[65]

Críticos do uso dessa medida também pontuaram preocupações sobre o risco de "sequestro de função", por meio do qual medidas são introduzidas exclusivamente para identificar imagens de abuso sexual infantil, mas são ampliadas de tal forma que levem a uma intrusão muito maior e a denúncias de atividades individuais - legais ou não - para as autoridades. Pesquisadores de Princeton, em 2021, interromperam seu próprio programa de escaneamento quando perceberam quão facilmente seu sistema

64 Leaked EU Commission working document: *Technical solutions to detect child sexual abuse in end-to-end encrypted communications*, 2020, https://www.politico.eu/wp-content/uploads/2020/09/SKM_C45820090717470-1_new.pdf

65 Entrevista de CRIN e ddm com Privacy International, 26 de setembro de 2022

poderia ser reaproveitado para vigilância e censura. "O design não era estrito para uma categoria específica de conteúdo; um serviço poderia simplesmente trocar a base de dados de correspondência de conteúdo e a pessoa utilizando aquele serviço não saberia de nada."[66] China e Índia aproveitaram tal tecnologia para esses objetivos[67], o que torna esse um risco muito real, e não apenas teórico.

Algumas propostas de implementação de escaneamento no dispositivo respondem em alguns aspectos a essa preocupação, avisando ao usuário quando uma correspondência é identificada e bloqueando o conteúdo, mas não notificando as autoridades. Mesmo nesse caso, alguns entrevistados foram cautelosos em relação ao sequestro de função: "Se as pessoas estão acostumadas a um sistema como esse funcionando em segundo plano em seus aparelhos, então quão difícil seria virar a chave e começar a denunciar para as autoridades? [...] É uma ferramenta muito poderosa e muitos governos ao redor do mundo que são mais repressivos vão querer ter acesso a ele e expandi-lo [para além de material de abuso sexual infantil]."[68]

> *"De uma perspectiva legal. você poderia tentar inserir controles e limites, mas o próximo governo pode ter visões diferentes e se livrar dessas amarras [...] Uma vez que a tecnologia está inserida, pessoas vão vir com todo tipo de ideia sobre como ela poderia ser utilizada para lidar com novos problemas sociais. [...] [Foi amplamente dito que] 'Código é lei', que tecnologia tem impacto legal. Eu atualmente penso que vai mais longe que isso. Acho que, em alguns aspectos, tecnologia é como o direito constitucional, que estabelece coisas que são muito difíceis de mudar depois. Quando cada iPhone e todo Android tiverem esse tipo de capacidade de escaneamento de CSAM, bem, por que os governos não deveriam pedir para começar a procurar por manuais de instrução para fabricação de bombas, imagens extremistas, e insultos a figuras religiosas?"*[69]

Dr Ian Levy, ex-diretor técnico do *National Cyber Security Centre* [Centro Nacional de Cibersegurança] (NCSC) e Crispin Robinson, diretor técnico para cripto análises no GCHQ, promoveram uma abordagem mais explícita à varredura pelo lado do cliente em artigo de julho de 2022, como uma forma de alcançar o mesmo objetivo em vigilância em massa e afirmam fazê-lo sem ameaçar a privacidade dos usuários. Outros discordam. Uma vez que essa interferência na privacidade é realizada em escala de populações inteiras, um grupo de especialistas líderes em segurança e criptografia a descreve como tecnologia de vigilância em massa no artigo *"Bugs in our Pockets"* publicado no verão[70] de 2021.[71]

66 9to5Mac, *Princeton University says it knows Apple's CSAM system is dangerous – because it built one*, 20 de agosto de 2021, https://9to5mac.com/2021/08/20/apples-csam-system-is-dangerous/

67 EFF, India's Draconian Rules for Internet Platforms Threaten User Privacy and Undermine Encryption, 20 de julho de 2021, https://www.eff.org/deeplinks/2021/07/indias-draconian-rules-internet-platforms-threaten-userprivacy-and-undermine

68 Entrevista de CRIN e ddm com Privacy International, 26 de setembro de 2022.

69 Entrevista de CRIN e ddm, entrevista com Ian Brown, 6 de outubro de 2022.

70 NT: o período "verão de 2021" faz referência aos meses de junho a setembro de 2021, que compreendem a estação do verão no hemisfério Norte.

71 Abelson, H. et al., *Bugs in our Pockets: The Risks of Client-Side Scanning*, 2021, https://arxiv.org/pdf/2110.07450.pdf



Eles explicaram porque isso torna o que era antes privado no dispositivo dos usuários em potencialmente disponível para as forças policiais e agências de inteligência, mesmo na ausência de um mandado.

> *"[Varredura pelo lado do cliente] nem garante eficácia na prevenção de crimes, nem previne vigilância. Na realidade, o efeito é o oposto. VLC, por sua natureza, cria sérios riscos à segurança e à privacidade de toda a sociedade, enquanto o auxílio que oferece às forças de segurança é, na melhor das hipóteses, problemático. Existem múltiplas formas pelas quais a varredura pelo lado do cliente pode falhar, ser evadida e abusada."*

O risco de sequestro de função cria uma questão real sobre o que limita a tecnologia de se tornar um tipo de reconhecimento facial para todos os propósitos e uma ferramenta de denúncia para o Estado? Já que alguns aspectos da legislação proposta na União Europeia tornariam a denúncia obrigatória, e nos Estados Unidos a denúncia de material de abuso sexual infantil para o NCMEC já é obrigatória[72], a questão que surge é se organizações envolvidas no monitoramento de denúncias, como o NCMEC, são inteiramente privadas ou se, no contexto legal, são um "ator estatal". Essa pergunta, por sua vez, levanta questões sobre escrutínio apropriado e fiscalização.

No relatório de agosto de 2022, O direito à privacidade na era digital, o Escritório do Alto Comissariado da ONU para os Direitos Humanos fez diversos comentários sobre da varredura pelo lado do cliente, afirmando que:

*"Varredura pelo lado do cliente também cria novos desafios de segurança, tornando violações de segurança mais prováveis."*[73]

*"A imposição generalizada de varredura pelo lado do cliente iria constituir uma mudança de paradigma que levanta uma gama de problemas sérios com consequências potencialmente terríveis para a vivência do direito à privacidade e de outros direitos. Diferente de outras intervenções, varredura pelo lado do cliente geral e obrigatória iria inevitavelmente afetar todos utilizando meios de comunicação modernos, não apenas pessoas envolvidas em crimes e sérias ameaças à segurança."*[74]
*"Dada a possibilidade de tais impactos, é provável que a vigilância indiscriminada gere um efeito inibidor significativo na liberdade de expressão e de associação, com pessoas limitando as formas como se comunicam e interagem com outras e se engajando em autocensura."*[75]

72 Rosenzweig, *The Law and Policy of Client-Side Scanning*, 20 de agosto de 2020, https://www.lawfareblog.com/law-and-policy-client-side-scanning

73 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/51/17, 4 de Agosto de 2022, para. 28, https://www.ohchr.org/en/documents/thematic-reports/ahrc5117-right-privacy-digital-age

74 Id., para. 27.

75 Ibidem

## Criptografia homomórfica e tecnologias emergentes

Criptografia homomórfica em dispositivos - uma forma de criptografia que permite usuários realizarem cálculos em dados criptografados sem descriptografá-los - com *hashing* e correspondência pelo lado do servidor já foi sugerida como uma tecnologia com potencial. A partir desse método, imagens são criptografadas utilizando um esquema criptográfico parcialmente homomórfico, cuidadosamente escolhido, que permite que uma versão criptografada do *hash* seja computada da imagem criptografada. As imagens criptografadas são enviadas para um servidor *online* do provedor de serviço para *hashing* e comparadas com uma versão criptografada da lista de *hash*. O servidor não tem as chaves criptográficas homomórficas, então não pode acessar os conteúdos da imagem, mas apenas pode identificar se há uma correspondência ou não no banco de dados das imagens. Se o banco de dados contém apenas um tipo de conteúdo de imagem, o provedor do servidor pode então inferir o que foi identificado no dispositivo dos usuários, mas não acessar a imagem em si.

Alguns entrevistados pensam que investir em tecnologias de proteção da privacidade como a criptografia homomórfica seria uma forma de avançar no debate.

> *"Nós tivemos conversas com parceiros da indústria e falamos, 'Vocês estão olhando para isso?', mas um dos comentários que recebemos de volta foi 'É muito caro'. [...] Na realidade, essa seria uma forma bem positiva de utilizar criptografia. Eu posso fazer correspondência de algo mesmo sem saber o que eu estou comparando e em relação a quê estou comparando. [...] É uma forma de usar criptografia para expor a menor quantidade de informações possível."*[76]

> *"Minha percepção geral é de que a tecnologia está ficando melhor e mais rápida. [...] Houve conversas teóricas sobre criptografia homomórfica, ou computação quântica, e como ela pode levar à capacidade de quebra da criptografia, mas eu penso que estamos muito longes dessas soluções. E quando chegarmos a esse ponto, também teremos uma criptografia mais poderosa."*[77]

Entretanto, acesso mais fácil a sistemas, redes e dispositivos, aumenta o risco de uso incorreto que a Agência da União Europeia para a Cibersegurança (ENISA)[78] vê que não pode ser combatido com tecnologia.
Pesquisa feita pela *Tech Against Terrorism* concluiu que a tecnologia não está completamente desenvolvida, e desenvolver esse tipo de soluções é caro. Ademais, elas apresentam riscos à segurança, levantam questões jurisdicionais, e violam a privacidade.[79]

76 Entrevista de CRIN e ddm com IWF, 3 de novembro de 2022.

77 Entrevista de CRIN e ddm com Privacy International, 26 de setembro de 2022.

78 ENISA, *Solving the Cryptography Riddle: Post-quantum Computing & Crypto-assets Blockchain Puzzles*, 2021, https://www.enisa.europa.eu/news/enisa-news/solving-the-cryptography-riddle-post-quantum-computing-crypto-assets-blockchain-puzzles

79 Tech Against Terrorism, *Terrorist Use of E2EE: State of Play, Misconceptions, and Mitigation Strategies*, 2021, p. 62.



O *Information Commissioner's Office* [autoridade de proteção de dados] do Reino Unido descreve quão importante é escolher o algoritmo correto e garantir que a chave tenha tamanho grande o suficiente para promover a defesa contra ataques durante todo ciclo da vida dos dados.[80] Conforme aumenta o poder do processamento computacional ou novos métodos de ataques matemáticos são descobertos, uma chave deve permanecer suficientemente grande para garantir que um ataque continue sendo praticamente impossível. A computação quântica cria novos riscos para cada forma prévia de criptografia.

De acordo com a ENISA, a tecnologia quântica irá "permitir um grande salto em muitos ramos da indústria, assim como pode eficientemente resolver problemas para os quais as tecnologias de hoje não são capazes de fornecer a solução. Entretanto, essa tecnologia será altamente disruptiva para os nossos padrões de segurança em equipamentos e sistemas. Cientistas concordam, em geral, que computadores quânticos serão capazes de quebrar chaves públicas amplamente utilizadas em sistemas criptográficos."[81]

## Acesso secreto a conteúdos em tempo real via escuta telefônica

Outra abordagem para acessar dados criptografados é por meio de monitoramento secreto. Vários termos são utilizados de forma intercambiável para descrever esse tipo de atividade, incluindo "acesso excepcional legal" e "*hacking legal*", mas a proposta mais conhecida é o chamado "protocolo fantasma". O que todas essas medidas têm em comum é que elas buscam ter acesso secreto a comunicações criptografadas.

O "protocolo fantasma",[82] do GCHQ propôs adicionar um terceiro, silencioso, a conversações criptografadas. Em termos simples, isso significa que as forças policiais ou de segurança nacional seriam capazes de acessar conteúdos discutidos em ambientes criptografados sem enfraquecer a criptografia em si, já que eles seriam parte da conversa. Essa medida tem sido amplamente condenada por grupos de tecnologia e privacidade, incluindo a *Internet Society.*[83] "Enquanto otimismo e cooperação são bons em princípio, parece improvável que provedores de comunicação vão voluntariamente inserir uma poderosa capacidade de escuta em seus sistemas criptografados, até porque essa seria uma modificação enorme e arriscada."[84]

80 UK Information Commissioner's Office, *Encryption*, 2022, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/encryption/#new

81 ENISA, *Solving the Cryptography Riddle: Post-quantum Computing & Crypto-assets Blockchain Puzzles*, 2021.

82 Levy, I. and Robinson, C., *Principles for a More Informed Exceptional Access Debate*, 2018.

83 Internet Society (ISOC), *Ghost Protocol Fact Sheet*, 2020.

84 Ibidem.

> *"Foi dito que o protocolo fantasma não quebra a criptografia - não pede a remoção da criptografia porque você está apenas adicionando um usuário invisível silencioso. [...] Mas, da nossa perspectiva, ele cria uma grande vulnerabilidade de segurança. [...] Esse fantasma é obviamente destinado à aplicação da lei, mas [...] criminosos podem conseguir acesso à tecnologia e Estados que não respeitam os direitos humanos podem forçar provedores de serviços a terem acesso às comunicações criptografadas sem o conhecimento dos participantes, e isso quebra a criptografia."*[85]

"*Hacking* legal" é outro meio de se ter acesso a ambientes criptografados. Tratam-se de medidas que tentam explorar vulnerabilidades de segurança para ganhar acesso a comunicações com criptografia ponta a ponta, seja intencionalmente criando uma fraqueza que autoridades sabem como acessar, seja tirando vantagem de um defeito não intencional na segurança.

> *"O que eles têm em comum, em última instância, é que ou exigem, ou tentam explorar vulnerabilidades. Na minha perspectiva, eles enfraquecem a própria essência da criptografia, qual seja de que nenhuma pessoa pode ter acesso à comunicação além do remetente e do destinatário. Então, é essencialmente criando uma vulnerabilidade no sistema que as forças da lei são capazes de acessá-lo. Agora, isso é o mesmo que construir uma casa e dizer que você pode ter uma tranca na porta da frente, mas que precisa ter uma porta dos fundos pela qual a polícia pode entrar a qualquer momento quando tiver uma ordem judicial, de forma que tudo que isso faz é criar uma oportunidade para que alguém a invada."*[86]

Alguns entrevistados argumentaram que o *hacking* legal deveria ser aceitável se estiver alinhado a salvaguardas extremamente rigorosas, por exemplo, a garantia de que não irá diminuir a segurança do dispositivo como um todo. De qualquer forma, um dos entrevistados aponta que "Governos já recebem acesso aos conteúdos de comunicações criptografadas por meio de ataques de força bruta ou empregando outras técnicas para burlar a criptografia. Tais medidas precisam ser reguladas, e combinadas com salvaguardas processuais e substantivas que balizem tais acessos, caso a caso."[87]

85 Entrevista de CRIN e ddm com Privacy International, 26 de setembro de 2022.

86 Entrevista de CRIN e ddm com Richard Wingfield, 6 de setembro de 2022.

87 Entrevista de CRIN e ddm com Centre for Democracy and Technology (Escritório da Europa), 13 de outubro de 2022.



Outros comentadores foram mais céticos sobre a possibilidade de alcançar esse tipo de acesso seguramente sem enfraquecer fundamentalmente comunicações criptografadas:

> *"Sabemos que hackers e pessoas que querem acessar comunicações criptografadas de indivíduos são experientes com tecnologia, e em muitos casos mais que instituições de aplicação da lei e segurança, então seria uma questão de tempo até que qualquer vulnerabilidade obrigatória fosse identificada por outros, de forma que você estaria constantemente jogando um jogo de gato e rato, consertando uma vulnerabilidade e criando uma nova. Então não acho que exista uma solução sustentável. É melhor que você não tenha criptografia em primeiro lugar se você vai ter uma vulnerabilidade nesse caso."*[88]

Na prática, forças policiais têm um número de ferramentas à sua disposição que funcionam como "*hacking* legal". *GrayKey* permite às forças de segurança recuperar dados de iOS e dos principais dispositivos Android, incluindo dados criptografados ou inacessíveis. O *Universal Forensic Extraction Device* [Dispositivo Universal de Extração Forense] da *Cellebrite*, *software* que extrai dados de dispositivos móveis e gera um relatório resumindo-os, é capaz de detectar e informar até mesmo dados excluídos. Outras ferramentas são coletores de IMSI, essencialmente uma torre de celular "falsa" que age entre o dispositivo celular do alvo e as torres reais dos provedores de serviços, o que é considerado um ataque por interceptação (*man-in-the-middle* - MITM). Essas soluções tecnológicas de alto custo são altamente procuradas e utilizadas pelos Estados. Enquanto alguns Estados já perceberam que essas medidas são politicamente impalatáveis ou ilegais, outros estão ignorando os princípios do Estado de Direito, democracia e direitos humanos, e contratando terceiros para fazer espionagem em seu nome.[89]

Pesquisadores descobriram na Nigéria que o governo aumentou seu gasto na última década com a aquisição de diversas tecnologias de vigilância e aprovou um orçamento suplementar para comprar ferramentas capazes de monitorar comunicações criptografadas do *WhatsApp*.[90]

88 Entrevista de CRIN e ddm com Richard Wingfield, 6 de setembro de 2022.

89 Por exemplo, o spyware israelense Pegasus do NSO Group, que esteve implicado no assassinato do jornalista saudita Jamal Khashoggi.

90 Oloyede, R. and Robinson, S., *Surveillance laws are failing to protect privacy rights: What we found in six African countries*, 26 de outubro de 2021, Institute of Development Studies, https://www.ids.ac.uk/opinions/surveillance-laws-are-failing-to-protect-privacy-rights-what-we-found-in-six-african-countries/; Premium Times, *Nigerian govt moves to control media, allocates N4.8bn to monitor WhatsApp, phone calls*, 12 de julho de 2021, https://www.premiumtimesng.com/news/headlines/473147-as-nigeria-moves-to-control-media-nia-gets-n4-8bn-to-monitor-whatsapp-phone-calls.html

### Acesso secreto a conteúdos em tempo real via *malware* e interceptação

É possível ter acesso à comunicação criptografada por meio da instalação de "*malware*" (*software* malicioso) no dispositivo. O exemplo de maior destaque tem sido o uso do "Pegasus", *software* desenvolvido pelo *NSO Group.* O *software* pode ser instalado no celular remotamente, sem que seu dono saiba, transformando o dispositivo em um aparelho de vigilância. O *software* é capaz de copiar mensagens que são enviadas ou recebidas, acessar fotos, ligar o microfone para gravar conversas, ligar a câmera e acessar localização.

Pesquisa feita pelo *Citizen Lab* em 2020 encontrou o que eles chamam de "um quadro sombrio de riscos aos direitos humanos pela proliferação global do NSO". Países onde há operações significativas do spyware Pegasus já haviam sido reportados por usos abusivos de *spyware* contra a sociedade civil, incluindo Bahrein, Cazaquistão, México, Marrocos, Arábia Saudita e Emirados Árabe Unidos. Em agosto de 2016, o ativista premiado emiradense Ahmed Mansoor foi infectado com o *spyware* Pegasus do *NSO Group*.[91]

Seja por solicitação, por meio de "interferência legal" aprovada ou por interferência governamental por meio de *hacking*,[92] uma vez que se tornam visíveis a uma empresa os conteúdos de comunicações, por extensão, o governo e as forças de segurança também passam a ter acesso a eles de maneiras que antes não teriam.

Essas ameaças são suplementares a ameaças internas. Em 2019, o Departamento de Justiça dos Estados Unidos indiciou dois ex-empregados do Twitter por acessarem informações pessoais de mais de 6000 contas do Twitter em 2015 em nome da Arábia Saudita.[93] Tecnologias de enclave seguro, que na prática são "configurações seguras" dentro de empresas a que nem todos os empregados têm acesso, são projetadas para mitigar, mas não resolvem esse problema.

Existe uma falta de confiança nos governos ao redor do mundo para que dados de comunicações dos seus opositores sejam utilizados incorretamente de diversas formas e maneiras. Quando não podem confiar no governo, indivíduos dependem dos direitos humanos fundamentais previstos em lei como um impeditivo de abusos e um caminho para reparação.

91 Marczak, B. et al., *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, 2018, Citizen Lab Research Report No. 113, University of Toronto, https://tspace.library.utoronto.ca/bitstream/1807/95391/1/Report%23113--hide%20and%20seek.pdf

92 UK Government, *National Cyber Force Transforms country's cyber capabilities to protect UK*, 19 November 2020, https://www.gov.uk/government/news/national-cyber-force-transforms-countrys-cyber-capabilities-to-protect-uk

93 Washington Post, *Former Twitter employees charged with spying for Saudi Arabia by digging into the accounts of kingdom critics*, 6 November 2019, https://www.washingtonpost.com/national-security/former-twitter-employees-charged-with-spying-for-saudi-arabia-by-digging-into-the-accounts-of-kingdom-critics/2019/11/06/2e9593da-00a0-11ea-8bab-0fc209e065a8_story.html



## Quebrando mitos da criptografia

"Quebrar" criptografia de dados em trânsitos e dos conteúdos das comunicações depende da capacidade de ler os conteúdos "em texto plano" e reuni-los da forma que o remetente desejava que o destinatário os lesse. Isso implica você obter a chave dada, encontrada, adivinhada ou entregue pelo destinatário, ou burlar a chave explorando uma falha para ter acesso aos conteúdos planos utilizados ou então localizando uma cópia deles. Qual método será utilizado depende de quem o está buscando, para qual tipo acesso e conteúdo e por quê. A avaliação da União Europeia de eficácia, viabilidade e riscos, assim como resultados de várias soluções alternativas, podem ser lidas na versão rascunho do relatório de trabalho da Comissão Europeia vazada em 2020.[94]

Conforme mais e mais conteúdos têm se tornado seguros em trânsito e com um aumento do uso de sistemas entre pares *(peer-to-peer)*, os pontos por meio dos quais terceiros podem mais facilmente acessar dados de comunicações são as pontas. O debate sobre criptografia de ponta a ponta, dessa forma se tornou mais tenso com o passar do tempo, com serviços de segurança, Estado, e forças de aplicação da lei sugerindo que mais segurança para os usuários torna o acesso por parte de serviços de segurança mais difícil. O empurrão, portanto, é por serviços que não precisam "quebrar a criptografia" onde ela é utilizada, mas sim que operam no dispositivo, ou então nos servidores que são pontas do processo. Ainda que essas técnicas não comprometam a arquitetura técnica de sistema de criptografia de ponta a ponta na totalidade, comprometem seu propósito e objetivo na prática.

O conceito de "quebrar criptografia" no contexto de detecção e aplicação da lei para proteção de crianças foi ultrapassado pelo amplo uso de uma abordagem alternativa: burlar a criptografia.[95] A tecnologia não necessita ser quebrada se, ao invés disso, o objetivo da criptografia de ponta a ponta for quebrado.

## Denúncia de usuários

Denúncia de usuários é amplamente reconhecida como uma parte vital de qualquer política e prática, seja por parte da empresa responsável pela identificação e derrubada de conteúdo, ou ao nível individual.

Por exemplo, o *WhatsApp* reporta todos os casos aparentes de exploração sexual infantil em seu serviço de qualquer parte do mundo para o NCMEC, de acordo com sua política publicada[96], incluindo via pedidos governamentais.

94 Leaked EU Commission working document: *Technical solutions to detect child sexual abuse in end-to-end encrypted communications*, 2020.

95 Kerr, O. S. and Schneier, B., *Encryption Workarounds*, 2017, 106 Georgetown Law Journal 989 (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2938033

96 Veja: https://faq.whatsapp.com/444002211197967/?locale=lv_LV

> *"Eu penso que denúncia do usuário é algo que deveria ser encorajado tanto quanto possível, assumindo que o que está sendo denunciado é comportamento ou material legitimamente ilegal. [...] A regulação é necessária para tornar mais fácil para usuários serem capazes de denunciar materiais e comportamentos que violam os termos de serviços das plataformas e para que se tenha processos mais claros e transparentes de avaliação feita pela empresa, e, em seguida, olhar para mecanismos de apelação, etc. Deveria ser tão fácil quanto possível, particularmente para crianças e outros usuários vulnerabilizados, reportar algo potencialmente danoso e entender as regras das plataformas usadas para denunciar atividade e comportamento ofensivo e ilegal de outras pessoas. [...] Crianças devem ser mais bem equipadas, já que estão crescendo usando essas tecnologias, para saber como utilizá-las seguramente, seja por meio das escolas, iniciativas das plataformas, ou por escolhas de design das próprias plataformas."*[97]

Denúncia de usuários por parte de indivíduos e coletivos organizados, é claro, também podem ser utilizadas contra pessoas de formas inesperadas e transformadas em arma de larga escala.

Usuários do *WhatsApp* utilizaram seu sistema de denúncia para atacar outros usuários de acordo com moderadores entrevistados pela *ProPublica*, que disseram, em 2021: "nós tivemos em alguns meses nos quais a IA estava banindo grupos de esquerda e direita" porque usuários no Brasil e México mudavam o nome do grupo para algo problemático e denunciavam mensagens. "No pior momento", lembra o moderador, "nós estávamos tendo por volta de dez mil desses casos. Eles descobriram algumas palavras das quais o algoritmo não gostava."[98]

Entretanto, a denúncia do usuário é uma das abordagens que não cria tensão entre privacidade e segurança em ambientes criptografados, tendo pouco ou nenhum desafio técnico. Entrevistados, especialmente aqueles envolvidos no suporte a vítimas e sobreviventes, frequentemente destacam que as denúncias de usuários foram inadequadamente conduzidas, com larga demora, às vezes de semanas, entre a denúncia e a derrubada do conteúdo. Isso se tornará cada vez mais política e publicamente inaceitável com uma pressão crescente nas empresas de redes sociais devido a novas legislações em todo o mundo.

---

97 Entrevista de CRIN e ddm com Richard Wingfield, 6 de setembro de 2022.

98 Ars Technica, *WhatsApp "end-to-end encrypted" messages aren't that private after all*, 8 September 2021, https://arstechnica.com/gadgets/2021/09/whatsapp-end-to-end-encrypted-messages-arent-that-private-after-all/

Resumo: Tecnologias discutidas no debate sobre combate à violência e exploração sexual de crianças

| | | Criptografia ponta a ponta em trânsito com extração de hash do conteúdo e correspondência no upload para o provedor de serviço ou servidores dos provedores | | | Métodos para burlar a criptografia ou explorar vulnerabilidades na segurança | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | *PhotoDNA* (apenas opera em ambientes sem criptografia, por exemplo na web aberta sem https e em canais sem criptografia ponta a ponta ou em pontos onde o conteúdo não é criptografado em repouso como no provedor de serviço) | Criptografia homomórfica no dispositivo com *hashing* de imagem e correspondência do lado do servidor | Ferramentas de escaneamento baseadas em texto (apenas operam em ambientes não criptografados por exemplo a web aberta e pontos não criptografados em canais de comunicação) | Detecção pelo lado do cliente no dispositivo com segunda etapa na nuvem de moderação baseada em imagem e texto | Enclaves seguros no servidor do provedor de serviço, com correspondência via criptografia homomórfica | Acesso aberto ao dispositivo com informação enviada para outro dispositivo (por exemplo produtos estilo "controle parental") | *Chips Key* Escrow no dispositivo em escala massiva (por exemplo *Clipper Chip*) | *Spyware* (acesso remoto secreto a dispositivos móveis não autorizado pelo dono do dispositivo por exemplo Pegasus) | *Hacking* no dispositivo (dispositivo físico acessado não autorizado pelo dono do aparelho, por exemplo *Cellebrite*) | Acesso pelo lado do servidor a todo conteúdo por design (por exemplo ferramentas estilo *man-in--the-middle*, incluindo produtos Child Safety Tech) | Protocolo fantasma (adicionando um terceiro à comunicação desconhecido pelo proprietário do dispositivo, por exemplo serviços de vigilância estatal) |
| **Características das ferramentas** | | | | | | | | | | | |
| Direcionado apenas aos indivíduos (pode ser aplicado em escala) | | | | | | X | | X | X | | X |
| Não direcionado | X | X | X | X | X | | X | | X | X | |
| Identifica conteúdo em ambientes criptografados | | X | | X | X | X | X | X | | | X |
| Permite vigilância em massa de conteúdos pelas empresas | X | X | X | X | X | | X | X | | X | X |
| Permite vigilância em massa de conteúdos pelos agentes de aplicação da lei / forças de segurança | X | X | X | X | X | | X | X | | X | X |
| Possível acesso excepcional por serviços de segurança estatal (sua legalidade depende da jurisdição) | X | X | X | X | X | X | X | X | X | X | X |
| Compatível com uma proibição geral de monitoramento | | | | | | | | | | | |
| **Aplicação da ferramenta** | | | | | | | | | | | |
| Imagens de CSAM previamente identificadas (recirculando) de crianças abaixo de 13 anos | X | X | | X | X | X | X | X | X | X | X |
| Imagens de CSAM previamente identificadas (recirculando) de crianças entre 13 - 18 anos. | X | | | X | X | X | X | X | X | X | X |
| Imagens de CSAM "desconhecidas" de crianças abaixo de 13 anos | | | | X | | X | X | X | X | X | X |
| Imagens de CSAM "desconhecidas" de crianças entre 13 a 18 anos. | | | | X | | X | X | X | X | X | X |
| Aliciamento online (grooming) em tempo real via câmera (vídeo | | | X | X | | X | X | X | X | X | X |
| Sextorsão em tempo real via câmera (vídeo) | | | X | X | | X | X | X | X | X | X |
| Conteúdo ilegal trocado em mensageria E2EE entre adulto e criança e adolescente (baseado em texto ou imagem) | | | X | X | X | X | X | X | X | X | X |

# Atritos e falhas: a busca por consenso

*"Há muito mais pontos em comum no debate do que talvez alguns de nós reconheçamos. [...] São nos detalhes que as coisas ficam mais complicadas"*[99]

O debate sobre criptografia já foi descrito como "termonuclear", com "emoções intensas em ambos os lados"[100]. Para ir além das divisões que existem atualmente em relação à criptografia, é necessário compreender os atritos, fraturas e falhas que existem nesse espaço, bem como onde há espaço para o consenso.

Este capítulo explora os temas que surgiram ao longo das entrevistas, conversas privadas e revisão da literatura que constituem a espinha dorsal deste relatório, com o intuito de compreender melhor as perspectivas e o pensamento sobre os direitos das crianças e a criptografia e identificar um caminho a ser seguido.

## A urgente necessidade de abordar o abuso e a exploração sexual infantil *online*

A discussão sobre a regulamentação adequada da criptografia e os desafios de prevenir e identificar o abuso e a exploração sexual de crianças online tornaram-se indissociáveis. Particularmente no contexto europeu e norte-americano, essa questão ocupa um ponto central nos processos de reforma legislativa e regulatória. É também nesse contexto que emergem muitas das tensões mais explícitas. No entanto, apesar delas, em toda a gama de entrevistas, conversas e literatura analisada como parte desta investigação, não houve dúvida de que o abuso e a exploração sexual de crianças online requerem medidas urgentes para proteger as crianças e garantir a responsabilização dos abusadores. Nos casos em que uma opinião contrária foi constatada, ela estava relacionada com as diferentes perspectivas sobre como alcançar essa proteção e como proteger os direitos humanos de forma mais ampla.

> *"Não é uma questão de: devemos proteger as crianças ou não? Concordamos plenamente com a necessidade de proteção.*[101]

> *"Todos nós queremos proteger as crianças. [...] A questão é que os meios para o fazer podem ser diferentes."*[102]

---

99 Entrevista de CRIN e ddm com WeProtect Global Alliance, 19 de agosto de 2022.

100 POLITICO, *Europe's thermonuclear debate on privacy and child sexual abuse*, 20 de novembro de 2020, https://www.politico.eu/article/europes-thermonuclear-debate-on-privacy-and-child-sexual-abuse-2/

101 Entrevista de CRIN e ddm com Electronic Frontier Norway, 15 de setembro de 2022

102 Entrevista de CRIN e ddm com ISOC, 30 de agosto de 2022.

Apesar desta concordância a nível fundamental, muitos entrevistados que refletiram sobre o debate público sobre criptografia e a exploração e abuso sexual de crianças online descreveram um ambiente que se tornou hostil e emotivo de uma forma que dificultou mudanças. Alguns participantes revelaram que durante conversas sobre os riscos da criptografia – particularmente no contexto do abuso infantil – testemunharam uma tendência ao afastamento de uma crítica direcionada a argumentos para críticas voltadas a denúncias mais pessoais relacionadas ao que muitos consideram posições insensíveis e imorais. Como salientou um entrevistado, *"raramente temos a oportunidade de ter um debate informado e diferenciado em torno do tema porque é algo muito emocional".*[103] Outros identificaram casos de "alarmismo" e "retórica" que são bastante inflamatórios, por vezes até tóxicos, no debate.

Essa tensão representa um risco já que pode impedir o envolvimento de diferentes áreas de especialidade que serão necessárias para abordar de forma significativa o abuso e a exploração sexual de crianças *online*. No entanto, apesar desse desafio, os entrevistados sentiram, de uma forma geral, que conversas relacionadas ao tema estão tomando um novo rumo e possibilitando um progresso. Nas palavras de um entrevistado: *"Parece que ambos os lados concederam terreno. Sinto-me um tanto otimista quanto chegar a um ponto onde haja mais compreensão de ambos os lados."*[104]

**Uma nota sobre a escala do abuso e exploração sexual de crianças online**

*"Os números parecem muito rasos quando na verdade há uma história muito mais robusta por trás deles."*[105]

*"Qual é um número aceitável de crianças vítimas de abuso sexual? Eu não acredito que essa seja uma pergunta que devemos estar fazendo."*[106]

IEm 2021, o NCMEC recebeu 29,3 milhões de denúncias de suspeita de exploração sexual infantil, 35% a mais do que em 2020. As denúncias fornecidas por prestadores de serviços eletrônicos incluíram 39,9 milhões de imagens, das quais 16,9 milhões de imagens eram únicas, e 44,8 milhões de vídeos, dos quais 5,1 milhões eram únicos.[107]

Dada a proeminência dos princípios da necessidade e da proporcionalidade no debate sobre criptografia e os direitos das crianças, existe uma tendência para recorrer a números para defender soluções específicas.

Os dados foram vistos como "vitais para permitir que as nações compreendam a extensão" do problema do material de abuso sexual infantil *online* e para defender o "aumento do investimento governamental" na sua abordagem.[108] Os dados também foram utilizados para discutir sobre a eficácia e a necessidade de ferramentas de detecção automatizadas e no alerta sobre as consequências de desligá-las.[109] Por exemplo, o NCMEC registou uma diminuição de 58% nas denúncias relacionadas à exploração sexual de crianças na UE quando a Diretiva relativa à Privacidade e às Comunicações Eletrônicas da UE entrou em vigor e antes da sua derrogação temporária,[110] a qual limitou a capacidade da indústria para detectar, denunciar e remover material de abuso sexual infantil.[111]

No entanto, os números não são tão úteis para fazer avançar o debate como podem parecer. Alguns temem que às vezes "as pessoas possam olhar para números que parecem grandes demais para que se pense a seu respeito".[112] De toda forma, os números atuais estão longe de representar fielmente o problema. Como explicou um entrevistado do NCMEC, a subnotificação é considerada um problema significativo, uma vez que as plataformas temem os riscos para a sua reputação caso realizem um grande número de denúncias: "há muitas empresas por aí que talvez estejam no bolso ou na bolsa de todos neste momento, e elas fazem pouquíssimas denúncias. Sabemos que isto não representa o que acontece nos seus serviços".[113] A tendência emergente de "sextorsão", uma "combinação de crime de colarinho branco e exploração sexual infantil[114] também complica o quadro, porque as plataformas de pagamento digital através das quais ocorre a troca entre o agressor e a criança não denunciam a atividade financeira como abuso sexual.

Por outro lado, às vezes considera-se que os dados não refletem verdadeiramente a natureza e a extensão do problema devido ao número de conteúdos duplicados em circulação. Por exemplo, um estudo realizado pela Meta sobre o conteúdo relatado ao NCMEC em outubro e novembro de 2020 revelou que "90% desse conteúdo era igual ou visualmente semelhante a conteúdo relatado anteriormente. Cópias de apenas seis vídeos foram responsáveis por mais da metade do conteúdo de exploração infantil que denunciamos nesse período",

103 Entrevista de CRIN e ddm com 5Rights, 5 de setembro de 2022

104 Ibidem.

105 Entrevista de CRIN e ddm com NCMEC, 3 de novembro de 2022.

106 Entrevista de CRIN e ddm com a IWF, 3 de novembro de 2022.

107 NCMEC, *CyberTipline 2021 Report*, https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata

108 Kardefelt-Winther, D. et al., *Encryption, Privacy and Children's Right to Protection from Harm*, 2020, UNICEF Office of Research – Innocenti Working Paper 2020-14, p. 9, https://www.unicef-irc.org/publications/pdf/Encryption_privacy_and_children%E2%80%99s_right_to_protection_from_harm.pdf

109 Dan Sexton (IWF), *Not all Encryption is the same: social media is not ready for End-to-End Encryption*, 14 de março de 2022, https://www.iwf.org.uk/news-media/blogs/not-all-encryption-is-the-same-social-media-is-not-ready-for-end-to-end-encryption/

110 Veja o capítulo sobre propostas legislativas recentes.

111 NCMEC, *Battle won but not the war in the global fight for child safety*, 11 de maio de 2022, https://www.missingkids.org/blog/2020/we-are-in-danger-of-losing-the-global-battle-for-child-safety

112 Entrevista de CRIN e ddm com NCMEC, 3 de novembro de 2022.

113 Ibidem.

114 Ibidem.

indicando que "o número de conteúdos não é igual ao número de vítimas, e que o mesmo conteúdo, potencialmente ligeiramente alterado, está sendo compartilhado de forma repetida".[115]

A esses pontos, os sobreviventes e os defensores da proteção infantil responderam com firmeza: "As pessoas assumem que isso é uma coisa boa, já que menos imagens são compartilhadas mais vezes. No entanto, isso não me oferece nenhum conforto. Se minha imagem for compartilhada uma vez, será horrível. Se minha imagem está sendo compartilhada 1.000 ou 10.000 vezes… devo me sentir melhor porque é a mesma imagem?",[116] e "Há algo de falso em dizer que é repetitivo. Não é. É sempre um crime novo, com um novo perpetrador e uma nova vitimização. É como se a humanidade estivesse perdida nesta conversa, certo?"[117]

Se for necessário apresentar números, talvez mais importante do que a quantidade total de denúncias seja o número de "denúncias significativas",[118] que fornecem informações que poderiam potencialmente salvar uma criança. Mas, de acordo com a entrevista concedida pelo NCMEC, muitas empresas fornecem, em vez disso, "apenas uma casca da denúncia"[119] , no que parece ser um exercício de ticar caixas.

Mesmo quando existe alguma concordância sobre a importância dos números e o que eles significam, não é claro até que ponto as denúncias levam à resolução efetiva dos crimes contra as crianças. No que diz respeito especificamente ao Reino Unido, a National Crime Agency [Agência Nacional do Crime] "recebeu 102.842 relatórios do NCMEC, mas alguns deles estavam incompletos ou, uma vez investigados, não foram considerados abuso infantil. Desses, 20.038 [relatórios] foram encaminhados às forças policiais locais e iniciaram (ou contribuíram para) investigações. No mesmo ano, mais de 6.500 pessoas foram detidas ou compareceram voluntariamente devido a crimes relacionados a abuso infantil e mais de 8.700 crianças foram salvaguardadas."[120] A resposta das forças de segurança nacionais "varia amplamente em consequência de limitações de capacidade e de recursos". Está longe de ser claro "quantas investigações e detenções derivam diretamente dos relatórios do NCMEC a nível global, ou quantas menos teriam sido feitas com a criptografia de ponta a ponta implementada".[121]

115 Meta, *Preventing Child Exploitation on Our Apps*, 23 de fevereiro de 2021, https://about.fb.com/news/2021/02/preventing-child-exploitation-on-our-apps/

116 CRIN and ddm interview with the Marie Collins Foundation, 22 de novembro de 2022.

117 CRIN and ddm interview with NCMEC, 3 de novembro de 2022.

118 Ibidem.

119 Ibidem.

120 Levy, I. and Robinson, C., Thoughts on child safety on commodity platforms, 2022, p. 3.

121 Kardefelt-Winther, D. et al., *Encryption, Privacy and Children's Right to Protection from Harm*, 2020, UNICEF Office of Research – Innocenti Working Paper 2020-14, p. 9.



## Privacidade e proteção

*"Na verdade, o desafio que temos aqui é: como salvaguardar as crianças, ao mesmo tempo que protegemos a privacidade e outros direitos fundamentais?"*[122]

*"Precisamos ter uma conversa equilibrada sobre todos os direitos que leve em conta a segurança e também a privacidade."*[123]

Um segundo ponto central em torno do qual se formou o debate foi a caracterização da regulação *online* como uma questão de "privacidade versus proteção", ou, por vezes, mais diretamente a "proteção das crianças versus privacidade dos adultos". Essa divisão, muitas vezes vista como o cerne das disputas em relação à criptografia, por vezes apareceu em comunicações voltadas à incidência política (*advocacy*) analisadas durante a pesquisa para este relatório, mas entre os entrevistados e em análises escritas mais aprofundadas, as questões relacionadas à privacidade e à criptografia raramente foram tratadas nesses termos.

Como seria de se esperar, a defesa do valor da privacidade na regulação da criptografia foi feita com força entre organizações e especialistas cujo trabalho se centra na privacidade, bem como entre aqueles que trabalham mais diretamente com tecnologia. Como disse um entrevistado: "Lutamos para proteger a privacidade porque sabemos que é um direito muito importante e, em muitos aspectos, um guardião de outros direitos. [...] Sob vigilância, as pessoas são reprimidas e os seus direitos são limitados [...] A privacidade é basilar para o funcionamento dos Estados e as violações a ela são muito, muito concretas e podem levar a enormes danos. [...] Sabemos por meio da história o quão perigoso é quando a nossa privacidade é invadida pelo Estado - ter direito à privacidade é uma questão de restaurar esse equilíbrio de poder."[124]

Essa perspectiva, no entanto, não se limitou às organizações focadas exclusivamente nos direitos de privacidade. Alguns defensores dos direitos das crianças sublinharam que, tanto no debate em torno da criptografia como de um modo mais geral, a privacidade é muitas vezes vista erroneamente como um domínio dos adultos. Eles consideraram esse um sintoma de uma falha geral na forma como os direitos das crianças são discutidos, que tende a considerar as crianças como "objetos de proteção em vez de sujeitos de direitos plenamente formados".[125]

A mesma pessoa entrevistada enfatizou que as crianças têm direito à privacidade, mas também acrescentou que é necessário haver uma melhor compreensão de como a privacidade impacta o seu desenvolvimento.[126]

122 CRIN and ddm interview with EDRi, 9 August 2022.

123 CRIN and ddm interview with IWF, 3 November 2022.

124 CRIN and ddm interview with EDRi, 9 August 2022.

125 CRIN and ddm interview with the Alana Institute, 22 September 2022.

126 See, for example, the idea that Art. 8 of the European Convention on Human Rights protects the right to personal development, whether in terms of personality or of personal autonomy: European Court of Human Rights (Registry), *Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence*, updated on 31 August 2022, p. 25, https://www.echr.coe.int/documents/guide_art_8_eng.pdf

Outra pessoa alertou que "se a privacidade for violada, especialmente durante a infância, quando aspectos-chave do psicológico e da vida emocional estão sendo desenvolvidos, pode comprometer a formação dos indivíduos sociais e políticos."[127] Outro indivíduo demonstrou a mesma preocupação, afirmando que "as crianças que estão sendo vigiadas sentem que não podem realmente se expressar livremente, de uma forma independente. E isso pode realmente afetar o seu desenvolvimento e a forma como expõem as suas personalidades no mundo."[128]

> *"[A privacidade] permite que as crianças desenvolvam a sua personalidade com segurança, para descobrirem quem são."*[129]

Muitos entrevistados enfatizaram que a privacidade permite o exercício de outros direitos, incluindo a proteção contra a violência, apoiando fortemente a ideia de que a privacidade tem um elemento de proteção. Este elemento de proteção foi particularmente sublinhado no que diz respeito a crianças de grupos desfavorecidos e marginalizados. Os entrevistados apontaram para a ligação estabelecida entre privacidade e segurança no Comentário Geral n.º 25 do Comitê das Nações Unidas sobre os Direitos da Criança[130], que afirma que "a privacidade é vital para a segurança das crianças".[131]

Os defensores da privacidade digital também sugeriram que a polarização "privacidade versus proteção" pode ser parcialmente devida a "uma percepção de que a privacidade é de alguma forma abstrata e hipotética, atrapalhando o direito concreto à proteção das crianças".[132] Eles estavam preocupados com a sugestão de que aqueles que não têm nada a esconder não devem temer o enfraquecimento da criptografia. A essa percepção eles responderam vigorosamente que a preferência pela encriptação das comunicações para mantê-las privadas não indica, por si só, qualquer atividade danosa. No geral, enfatizaram fortemente a importância da privacidade como um direito fundamental que não é inferior ou secundário à proteção.

Uma das aplicações mais controversas do direito das crianças à privacidade que emergiu desta investigação foi a dos sobreviventes de abuso sexual infantil. Vários defensores da proteção infantil argumentaram que tende a haver uma visão unilateral da privacidade no debate em torno da criptografia, que trata a encriptação como totalmente positiva em termos de promoção da privacidade. Consideram que é dada muito pouca atenção à forma como a criptografia ameaça a privacidade daqueles que foram abusados sexualmente: "E quanto aos direitos das vítimas cujas imagens estão sendo difundidas por meio de canais encriptados? E os sobreviventes que sabem que as suas imagens foram repetidamente compartilhadas?"[133]

127 Resposta fornecida por Bits of Freedom ao questionário de CRIN e ddm.

128 Entrevista de CRIN e ddm com Instituto Alana, 22 de setembro de 2022

129 Resposta fornecida por Bits of Freedom ao questionário de CRIN e ddm.

130 N.T.: recomendamos a versão em português do comentário geral nº 25 traduzida pelo Instituto Alana: https://criancaeconsumo.org.br/wp-content/uploads/2022/01/comentario-geral-n-25-2021.pdf Há também uma versão comentada do documento produzida pelo mesmo instituto: https://alana.org.br/wp-content/uploads/2022/04/CG-25.pdf

131 Comitê dos Direitos da Criança da ONU, Comentário Geral No. 25 (2021) sobre os direitos da criança em relação ao ambiente digital, CRC/C/GC/25, 2 de março de 2021, § 67, https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en

132 Entrevista de CRIN e ddm com EDRi, 9 de agosto de 2022.

133 Entrevista de CRIN e ddm com ECPAT, 23 de agosto de 2022.



> *"Não sei quem viu minhas imagens, não sei quem as verá. Não quero que ninguém as veja."*[134]

Uma pessoa entrevistada que experienciou exploração e abuso sexual infantil online enfatizou que "para proteger a privacidade das crianças, precisamos ser capazes de identificar e remover imagens [de abuso *online*]", e ainda acrescentou que gostaria que todos os envolvidos, desde empresas de tecnologia a autoridades, fizessem "tudo o que fosse possível para obter essas imagens antes que alguém as visse".[135]

Em todo o espectro de entrevistados que participaram nesta pesquisa, o foco e a ênfase nas questões de privacidade abordadas variaram significativamente, mas houve um reconhecimento partilhado de que a privacidade das crianças é importante e é uma preocupação legítima na regulação da criptografia.

**Compreendendo a perspectiva das crianças sobre a privacidade**[136]

Pesquisadores que trabalham com crianças já alertaram que "é vital não confundir contextos interpessoais com contextos institucionais e comerciais para a privacidade, pois esses contextos diferem enormemente entre si quanto a de quem ou sobreo quê se busca privacidade". Eles salientaram que no discurso comum sobre privacidade e crianças, por exemplo, quando se vê que as crianças não têm um sentido de privacidade porque partilham informações pessoais livremente com outras pessoas, ou quando os pais estão preocupados com o aliciamento, "o foco é a privacidade interpessoal das crianças e suas implicações para a segurança". As crianças tendem, então, a "(excessivamente) estender o que sabem sobre relações interpessoais ao funcionamento das plataformas. Por exemplo, elas podem falar com confiança sobre o Instagram porque o pai de fulano trabalha com tecnologia e ele certamente 'jogaria limpo'. Elas assumem a reciprocidade ética: se nunca rastreariam alguém sem o seu conhecimento ou manteriam imagens contra a vontade de alguém, por que uma empresa o faria?" As crianças também parecem assumir que a forma como mantêm as suas informações privadas de outras pessoas (pseudônimos, modo fantasma, pesquisa anônima, limpeza do histórico) também as mantém privadas em relação às empresas.

Quando jovens entre 11 e 16 anos no Reino Unido foram incentivados, em *workshops*, a pensar para além da segurança eletrônica e para a forma como os dados são processados pelas escolas, médicos, ferramentas de busca e redes sociais, sua atitude mudou. "Suas expressões confiantes de agência e experiência vacilaram, e eles diziam, indignados: é assustador, as plataformas não deveriam bisbilhotar os contatos *online*, quero controlar com quem eles compartilham meus dados e, sobretudo, não é da conta deles!"

134 Entrevista de CRIN e ddm com a Fundação Marie Collins, 22 de novembro de 2022.

135 Ibidem.

136 Este texto é baseado em descobertas e citações de: Prof Sonia Livingstone OBE, "It's None of Their Business!" Children's Understanding of Privacy in the Platform Society, 2020 https://freedomreport.5rightsfoundation.com/its-none-of-their-business-childrens-understanding-of-privacy-in-the-platform-society

## Criptografia e as vozes dos sobreviventes de abuso sexual infantil

*"É muito fácil para as pessoas fazerem suposições sobre o que gostaríamos ou diríamos."*[137]

Numa pesquisa global de 2021 sobre violência sexual, 54% dos inquiridos afirmaram ter sofrido danos sexuais *online* quando crianças.[138] Mas os sobreviventes não constituem um grupo uniforme; eles são diversos, têm experiências variadas e pontos de vista variados sobre todas as questões, incluindo criptografia e abuso sexual infantil *online*.

Ao interagir com os sobreviventes ao longo desta investigação, alguns consideraram que já existe uma atenção significativa à privacidade - embora não necessariamente na privacidade das vítimas e dos sobreviventes -, mas que ainda não há um foco suficiente na segurança *online*. Houve um reconhecimento de que existe um consenso sobre a natureza terrível do abuso e da exploração sexual de crianças *online* e um desejo de endereçar esses temas e que os direitos das vítimas e sobreviventes devem ser respeitados quando buscamos alcançar tal objetivo. No entanto, uma preocupação que surgiu durante as entrevistas foi a de que a gravidade e a urgência do abuso *online* podem ser subestimadas na forma como a questão é discutida. Como explicou um entrevistado: "Muitas pessoas não compreendem completamente a natureza daquilo com que estamos lidando aqui, a sofisticação dos agressores [...] E a maioria delas nunca teve de lidar com vítimas ou sobreviventes."[139]

Vários participantes identificaram exemplos evidentes de culpabilização das vítimas, especialmente em discussões públicas. Por exemplo, um entrevistado expressou a sua consternação pela forma como um programa de revista de rádio apresentou a questão como "perpetradores que preparam crianças online e as coagem a abusarem sexualmente de si próprias".[140]"Agora pense nessa linguagem, pense nela. Estamos falando dos direitos das crianças. O seu direito a serem salvaguardadas é fundamental. E, na verdade, é nosso dever como adultos proteger as crianças. As crianças não andam por aí abusando sexualmente de si mesmas. Então, por onde começamos com os direitos das crianças? Precisamos começar com a linguagem."[141]

Muitos entrevistados argumentaram que as vozes das vítimas e dos sobreviventes deveriam ser mais ouvidas no debate. Enfatizaram que, embora existam organizações de dimensão considerável que defendem o benefício daqueles que são ou foram vítimas de abuso, muito raramente são realmente lideradas por pessoas com experiência vivida. "Precisamos encontrar uma maneira de incluir as vozes das vítimas e dos sobreviventes. Pura, não diluída ou interpretada. [...] Já vi muitos profissionais por aí se autodenominando 'consultores de sobreviventes' ou 'consultores de salvaguarda com experiência no trabalho com vítimas e sobreviventes' sendo consultados por [empresas de tecnologia] [...] Isso é de segunda mão, é a visão daquela pessoa sobre isso, através da sua filtragem, com o seu preconceito. Não é a voz verdadeira e pura da vítima e do sobrevivente."[142]

Um sobrevivente explicou: "A minha voz foi ouvida neste debate porque decidi falar abertamente. Entretanto não ouço, não vejo muitas outras pessoas com experiência vivida tendo a oportunidade de fazer isso [...] Houve algum envolvimento [com empresas de tecnologia], mas foi iniciado por mim. Ainda é, se assim posso dizer, bastante defensivo o lado da tecnologia. Não colaboram de forma alguma com as vítimas e sobreviventes, o que é bastante decepcionante porque é um grande problema para nós."[143]

Esse consenso sobre a necessidade de uma inclusão significativa dos sobreviventes nos processos de reforma foi claro e inequívoco, mas não foi uma simples expressão de apoio a qualquer resultado específico. Alguns sobreviventes de abuso sexual infantil enfatizam a necessidade de um desenvolvimento tecnológico mais forte para lidar com material de abuso sexual infantil online. Como explicou um entrevistado: "Para mim, o objetivo final seria que o conteúdo fosse pré-selecionado antes de ser carregado ou compartilhado. Dessa forma, não estará na plataforma, não verá a luz do dia."[144] Outras pessoas com experiência vivida, por outro lado, são defensores ferrenhos da privacidade e consideram ofensivo que sobreviventes de abuso estejam sendo usados - como assim o veem - para "promover uma agenda de vigilância política". Eles temem que as atuais propostas para proteger as crianças online deixem a porta aberta ao abuso de poder e possam empurrar para a clandestinidade atividades danosas, tornando sua detecção mais difícil.[145]

## O papel, possibilidades e limitações da tecnologia

*"Este é um debate sobre tecnologia e sociedade que não temos tido até agora [...] O que aconteceu com a tecnologia, o que aconteceu com a internet [...] e você chega a um ponto de crise em que não sabemos como realizar esse debate, e é aí que surge a polarização."*[146]

*"É um mito que se apenas fizermos a lei, os tecnólogos descobrirão um jeito."*[147]

137 Entrevista de CRIN e ddm com a Fundação Marie Collins, 22 de novembro de 2022.

138 WeProtect Global Alliance, *Global Threat Assessment* 2021, p. 6, https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2021.pdf

139 Entrevista de CRIN e ddm com a WeProtect Global Alliance, 19 de agosto de 2022.

140 O programa era Woman's Hour na BBC Radio 4, 18 de novembro de 2022, https://www.bbc.co.uk/sounds/play/m001f5fg

141 Entrevista de CRIN e ddm com a Fundação Marie Collins, 22 de novembro de 2022.

142 Ibidem.

143 Ibidem.

144 Ibidem.

145 Alexander Hanff, *Why I don't support privacy invasive measures to tackle child abuse*, 11 de novembro de 2020, https://www.linkedin.com/pulse/why-i-dont-support-privacy-invasive-measures-tackle-child-hanff

146 Entrevista de CRIN e ddm com a ECPAT, 23 de agosto de 2022.

147 Entrevista de CRIN e ddm com a Privacy International, 26 de setembro de 2022.

O papel e o potencial da tecnologia no combate ao abuso sexual infantil online atravessa o debate sobre como regular o espaço digital de forma que respeite os direitos humanos e ocupa um lugar de destaque nas entrevistas realizadas como parte da pesquisa para este relatório.

Houve consenso em todo o espectro de entrevistados sobre o papel central da tecnologia na abordagem desta questão. Os entrevistados que abordaram a questão numa perspectiva de proteção da criança reconheceram que o abuso sexual infantil é um problema complexo com muitas causas, mas sublinharam que a tecnologia desempenha um papel fundamental no problema. A tecnologia facilita diretamente o abuso, permitindo a propagação de material de abuso sexual infantil numa escala muito maior do que era possível antes. Mais indiretamente, pode também contribuir para uma cultura de normalização do abuso e da sexualização das crianças. Com base nessa perspectiva, tais entrevistados argumentaram que o forte aspecto tecnológico deve ser abordado e soluções técnicas, desenvolvidas.[148]

Vários entrevistados consideraram que o foco na tecnologia flui naturalmente, pelo menos em parte, como consequência dos esforços dos defensores da privacidade para encontrar a opção menos intrusiva em termos de interferência no direito à privacidade. Sugerindo um caminho a seguir, um entrevistado analisou o problema desta forma: "Não consigo pensar em nada mais necessário do que proteger uma criança da exploração e do abuso sexual. Então vamos fazer esse debate. Procuremos tecnologias que possam fazer incursões legítimas na privacidade, mas que não prejudiquem a essência desse direito."[149]

Ao procurar essas soluções, alguns sugeriram que as empresas, especialmente aquelas que são muito grandes e politicamente influentes, poderiam pesquisar novas tecnologias, consultar os governos sobre como seriam essas tecnologias na prática e talvez até chegar a um ponto em que possam testar algumas das afirmações empíricas feitas.[150]

Houve também uma nota de cautela, no entanto, por parte de algumas organizações que trabalham na questão a partir de uma perspectiva dos direitos das crianças, de que a tecnologia não pode ser uma solução mágica, mas que dado o ritmo da mudança no mundo digital, são sim necessárias algumas soluções tecnológicas: "Nós precisamos garantir que temos à nossa disposição ferramentas tão boas e tão modernas quanto o ambiente em que as crianças estão inseridas".[151]

A cautela em exagerar o papel potencial da tecnologia encontrou a sua expressão mais forte entre aqueles que alertaram contra o "tecnossolucionismo". Eles alertaram

148 Estas questões foram levantadas principalmente na entrevista de CRIN e ddm com a WeProtect Global Alliance, 19 de agosto de 2022

149 Entrevista de CRIN e ddm com um representante da sociedade civil, 12 de agosto de 2022.

150 Alguns destes pontos foram levantados na entrevista de CRIN e ddm com Ian Brown, 6 de outubro de 2022.

151 Entrevista de CRIN e ddm com Instituto Alana, 22 de setembro de 2022.



para as limitações da capacidade da tecnologia em resolver um problema tão complexo como o abuso sexual infantil online, ao mesmo tempo que protegendo os direitos fundamentais.

Uma preocupação significativa que emergiu das entrevistas foi que o foco na tecnologia - e em tecnologias específicas no contexto da criptografia - como solução corria o risco de ofuscar a natureza da questão mais ampla.[152] Uma pessoa entrevistada enquadrou a criptografia como uma parte terciária da discussão. Ela identificou o nível primário como sendo uma compreensão detalhada e abrangente do problema do abuso sexual de crianças online e a definição dos resultados que devem ser alcançados ao lidarmos com o abuso. A um nível secundário, a pessoa enxergou uma variedade de soluções, algumas de natureza tecnológica e outras não, que poderiam resolver aspectos do problema. Considera que a criptografia, especialmente a criptografia de ponta a ponta, entra em jogo num terceiro nível de equilíbrio das soluções possíveis e de decisão sobre aquelas que são as mais eficazes. Outro indivíduo entrevistado argumentou de forma semelhante: "Precisamos reformular o debate: o que estamos realmente tentando alcançar? Diferentes opções políticas podem ser usadas para tentar alcançar resultados diferentes [...] Identificar imagens é apenas um meio para um fim. Um número maior de imagens não é realmente uma métrica chave para determinar o sucesso ou o fracasso."[153]

Um tema relacionado que surgiu foi um desafio à ideia de que a tecnologia pode ser uma solução rápida. Houve preocupações de que essa ideia pudesse levar a reivindicações amplas, sem as devidas evidências, sobre o que várias propostas técnicas podem alcançar em termos de precisão e segurança, e até que ponto são compatíveis com a preservação de direitos. Um participante afirmou: "Há um foco excessivo na criptografia, no sentido de 'não podemos fazer muito contra o abuso por causa da criptografia' [...] e uma crença excessiva no que a tecnologia é capaz de alcançar."[154] Outro concluiu: "É um mito que se apenas fizermos a lei, os tecnólogos descobrirão um jeito."[155]

Essa expressão dos limites daquilo que a tecnologia é capaz de alcançar para abordar o abuso e a exploração sexual de crianças online foi mais claramente afirmada ao examinar propostas tecnológicas específicas:

> *"A tecnologia de prevenção ainda não existe. Quando olhamos para coisas como o aliciamento, por exemplo, a noção de tentar prever que linguagem alguém poderá usar... se não podemos fazer isso na vida real, o que não podemos - infelizmente não podemos prever que linguagem alguém com essa intenção usaria -, então a tecnologia também não pode fazer isso porque os dados e as informações obviamente têm que vir do mundo real. Por isso, eu diria definitivamente que, no que diz respeito à prevenção, é particularmente duvidoso recorrer à tecnologia para encontrar uma solução."*[156]

152 Conversa entre CRIN e ddm com representante da sociedade civil, 1 de junho de 2022.

153 Entrevista de CRIN e ddm com 5Rights, 5 de setembro de 2022.

154 Entrevista de CRIN e ddm com EDRi, 9 de agosto de 2022.

155 Entrevista de CRIN e ddm com a Privacy International, 26 de setembro de 2022.

156 CRIN and ddm interview with the Centre for Democracy and Technology (Europe Office), 13 October 2022.

Entre os entrevistados que foram críticos ou cautelosos sobre as possibilidades da tecnologia para abordar o abuso e a exploração sexual de crianças online, surgiu um debate substancial sobre ao papel que tecnologias específicas poderiam desempenhar e quem pode ter um papel legítimo no emprego dessas tecnologias.

## O papel da aplicação da lei

Um entrevistado que abordou esta questão a partir da perspectiva do direito à privacidade, explorou o potencial para o uso de tecnologia e poderes já existentes, que não exigiriam mais legislação ou regulamentação em muitas jurisdições:

> *"[A]qui existem muitas investigações de base tecnológica técnicas atualmente às quais as autoridades têm acesso e que não exigem a quebra da criptografia. Assim, por exemplo, se tiverem um suspeito específico, podem obter um mandado para apreender o seu dispositivo e depois ver o que está no próprio dispositivo. Ou podem obter um mandado para analisar os metadados de comunicações específicas."*[157]

Esta abordagem que se baseia na utilização dos poderes de aplicação da lei pelas autoridades responsáveis foi um tema comum em várias entrevistas. No entanto, um desafio colocado no contexto do abuso e exploração sexual de crianças *online* foi entender a escala do abuso. Olhando para a onipresença da Internet e a proliferação de material ilegal, alguns entrevistados explicaram que "você percebe que não pode moderar o conteúdo apenas com a verificação das pessoas", e que é necessária alguma intervenção intensiva na forma de automação.[158]

Para alguns, esse desafio é inevitável se a questão for tratada como sendo de competência das forças policiais. Outros questionaram esse enquadramento, argumentando em particular que a narrativa do "perigo estranho" não é apoiada em evidências.[159] Outros argumentaram, ainda que se o abuso sexual infantil é mais frequentemente perpetrado não por estranhos, mas por membros da família e outras pessoas conhecidas das crianças, como professores e figuras religiosas, então as propostas para proteger as crianças poderão ter de se concentrar mais no papel das forças policiais em identificar esses perpetradores, e menos na utilização da automatização para detectar material de abuso sexual infantil em todas as comunicações privadas. Outros, por vezes reconhecendo os perigos de confiar demasiadamente na narrativa do "perigo do estranho", manifestaram cautela em relação à capacidade das autoridades responsáveis pela aplicação da lei de cumprirem o seu papel em geral.

Uma das pessoas entrevistadas do Reino Unido, que trabalha neste espaço há quase 25 anos, disse: "O serviço policial deteriorou-se nos últimos 10 anos [...] A polícia estava melhorando bastante, mas, infelizmente, isso retrocedeu. E isso, penso eu, é principalmente resultado da falta de financiamento e da demissão de agentes mais experientes porque são mais caros [...] Mas a experiência é extremamente valiosa, trata-se de orientar novos agentes, etc."[160] A pessoa entrevistada também enfatizou a importância de investir na oferta de um nível padrão de treinamento para as autoridades policiais: "Algumas equipes com as quais lidei foram absolutamente péssimas. Algumas foram absolutamente fantásticas. Então é meio que uma loteria."[161]

O treinamento foi enfatizado como particularmente importante para quando os agentes policiais necessitam falar diretamente com crianças que são potenciais vítimas de abuso. Outro entrevistado residente no Reino Unido explicou a falta de sensibilidade e de técnicas de entrevista baseadas em traumas: "Eles são chamados à escola porque a criança tem uma imagem no telefone. Como conduzir essa conversa? Eles não sabem. E não é porque não queiram saber, é porque estamos abarrotando a sua formação com informações num período tão curtode tempo."[162] Um participante alertou que, se faltam fundos no que diz respeito a características básicas como a formação de oficiais, não se poderia esperar que a polícia fosse capaz de aplicar métodos de investigação mais inovadores, por exemplo, disfarçando-se em jogos de vídeo e utilizando o microfone e o chat do jogo para falar com as crianças de forma confidencial e identificar casos de abuso.[163]

Essa avaliação de uma deterioração na capacidade de forças policiais em lidar com o abuso e a exploração sexual de crianças também foi recebida com uma cautela relativamente ao empoderamento excessivo das entidades responsáveis pela aplicação da lei:

> *"Há uma tendência abrangente em toda a região europeia e a nível mundial de um aumento do poder das forças de segurança e uma diluição dos freios e contrapesos desse poder."*[164]

Tal preocupação ficou particularmente evidente nas discussões sobre crianças marginalizadas, que são mais propensas a ter experiências negativas de policiamento, incluindo racismo. Alguns participantes alertaram que a vigilância policial das comunidades desfavorecidas, possibilitada pela tecnologia, agravaria a injustiça e contribuiria para uma sensação de impunidade.[165] Uma das pessoas entrevistadas viu uma falta de consistência a nível europeu nas discussões sobre a aplicação da lei e a inteligência artificial. De um lado, tecnologias para detecção de abuso sexual

157 CRIN and ddm interview with Privacy International, 26 September 2022.

158 CRIN and ddm interview with IWF, 3 November 2022.

159 WeProtect Global Alliance, Global Threat Assessment 2021, p. 6.

160 Entrevista de CRIN e ddm com One in Four, 14 de novembro de 2022.

161 Ibidem.

162 Entrevista de CRIN e ddm com a Fundação Marie Collins, 22 de novembro de 2022.

163 Um exemplo dado foi o projeto Undercover Avatar da associação de proteção à juventude L'Enfant Bleu: https://www.cresta-awards.com/?action=ows:entries.details&e=97352&project_year=2022

164 Entrevista de CRIN e ddm com Centro para a Democracia e a Tecnologia (Escritório da Europa), 13 de outubro de 2022.

165 Para uma discussão sobre os riscos colocados pelas abordagens ao policiamento baseadas em dados, consulte: BBC, Civil liberties group afirma que os dados não são uma solução mágica para reduzir a criminalidade, 24 de novembro de 2022, https://www.bbc.com/news/uk-england-oxfordshire-63730451

infantil, do outro "eu diria que há um acordo muito forte neste momento [em relação à proposta da Lei de IA da UE] de que a implantação de IA pelas autoridades policiais é de alto risco e precisa ser fortemente regulamentada. Portanto, é extraordinário que na [proposta de Regulamento CSA da UE] tenhamos autoridades policiais usando diferentes graus de IA com as crianças mais vulneráveis".[166]

## O ecossistema mais amplo

As limitações das tecnologias de detecção e as restrições práticas sobre o que a aplicação da lei pode alcançar mesmo com essas tecnologias levaram vários entrevistados a pedir por uma abordagem sistêmica para o problema do abuso sexual infantil online. Como explicou um participante: "Quanto mais aprendemos sobre isso, mais percebemos que requer muitas intervenções diferentes. [...] Não existe uma coisa mágica. Você deveria estar fazendo de tudo."[167]

Uma oportunidade de consenso surgiu entre os entrevistados quando o valor e os méritos de qualquer aplicação tecnológica específica foram contextualizados.

> *"O design do sistema e o design dos serviços também desempenham um papel importante. E, de fato, muitos destes serviços poderiam fazer ajustes relativamente pequenos - se os adultos podem contatar diretamente as crianças, se podem fazer amizade ou seguir uma criança - vocês sabem, alguns projetos desse tipo, como forma de impedir caminhos de aliciamento."*[168]

Tal reconhecimento de que nenhuma aplicação individual de tecnologia impedirá e garantirá reparação pelo abuso e exploração sexual de crianças online, mas que muitos pequenos ajustes em conjunto podem ser eficazes, estabelece um espaço onde o potencial de consenso pode ser explorado.

Para além da prevenção desde a concepção e da interligação do espaço online, muitos participantes enfatizaram a necessidade de prestar mais atenção aos vários atores do ecossistema mais amplo. Alguns sugeriram que o foco excessivo na busca de uma solução tecnológica mágica é um produto da política: é mais conveniente apresentar propostas para combater os abusos sem aparentemente violar os direitos humanos do que reconhecer que ainda há muitas questões sem resposta e que soluções eficazes a longo prazo para o que é um problema social são difíceis de alcançar.

Por isso, várias pessoas entrevistadas apelaram a conversas honestas sobre a necessidade de investimento estatal e empresarial a vários níveis. Identificaram as escolas e o setor da saúde como intervenientes vitais e sugeriram que deveria haver um maior enfoque em: letramento digital, especialmente entre os jovens,

166 Entrevista de CRIN e ddm com Centro para a Democracia e a Tecnologia (Escritório da Europa), 13 de outubro de 2022.
167 Entrevista de CRIN e ddm com a IWF, 3 de novembro de 2022.
168 Entrevista de CRIN e ddm com 5Rights, 5 de setembro de 2022.



para os fazer compreender melhor os riscos de gerarem materiais por si próprios e de os compartilharem com pessoas que conhecem; sensibilizar os pais sobre como a tecnologia pode ser utilizada pelos seus filhos, bem como equipar melhor os médicos e outros profissionais de saúde para identificar os sinais físicos e psicológicos de abuso.

> *"Assistentes sociais, professores, todos nós estamos decepcionando as vítimas e os sobreviventes. E isso não é porque não temos vontade [de lutar contra o abuso], é porque não temos recursos para isso."*[169]

> *"Não tive acesso à terapia por nove anos após a minha experiência [de abuso]. Isso não é ok. Também é necessário que haja recursos investidos na recuperação."*[170]

Os serviços sociais, em particular, foram o foco de algumas discussões enérgicas em entrevistas. Uma clara necessidade de investimento foi identificada por muitos. Como explicou um entrevistado que trabalhou como assistente social no setor público do Reino Unido antes de fazer a transição para o setor de caridade: "Eu não poderia fazer a diferença no nosso clima político. Assistentes sociais experientes estavam partindo aos montes. Os bons seguiam outros caminhos. [...] Sempre que você tem austeridade, a primeira coisa que é cortada é treinamento. A segunda é o ânimo do pessoal."[171] Uma área particularmente importante que merece consideravelmente mais atenção são os serviços de recuperação, como apontado por um entrevistado com experiência vivida.[172]

Todos estes investimentos, como foi apontado em algumas entrevistas, deveriam ser complementados por pesquisas mais aprofundadas sobre o que impulsiona o comportamento dos abusadores, começando, por exemplo, com um verdadeiro questionamento acerca do fenômeno da sexualização das crianças, que - como sublinharam alguns sobreviventes - tem sido extremamente lucrativo para as indústrias da publicidade, da moda e do entretenimento.[173] Alguns também sugeriam que deveria ser feitas intervenções em infratores conhecidos enquanto eles estão encarcerados ou em liberdade condicional, e houve um foco muito mais forte na reabilitação no sistema de justiça criminal.

## Para além da autorregulação

O papel das plataformas digitais – particularmente, mas não exclusivamente, das grandes empresas de tecnologia – tem feito parte do debate sobre a regulação da internet há décadas. Diversas opiniões surgiram dos entrevistados que participaram no processo de pesquisa para este relatório sobre a melhor forma de alcançar uma regulação *online* eficaz, mas, de princípio, houve um grande consenso.

169 CRIN and ddm interview with the Marie Collins Foundation, 22 November 2022.
170 Ibidem.
171 Ibidem.
172 Ibidem.
173 Alexander Hanff, *Why I don't support privacy invasive measures to tackle child abuse*, 11 November 2020.

Houve um amplo acordo de que, ao abrigo das normas internacionais de direitos humanos, os Estados têm o dever de respeitar, proteger e cumprir com os direitos das crianças, também em relação ao que se aplica no contexto das atividades empresariais.

Houve também um consenso geral de que o impacto que as plataformas têm na sociedade é tão significativo que a era da autorregulação acabou. Como argumentou um entrevistado: "É necessário haver um certo grau de supervisão, e a supervisão democrática é preferível em muitos casos."[174]

Houve também consenso de que existe uma falta de uniformidade ou transparência no que diz respeito à forma como as plataformas lidam com o material de abuso sexual infantil na ausência de regulação. Entrevistados perceberam uma discrepância que deveria ser abordada e identificaram a necessidade de orientações claras às empresas para lhes dizer o que se espera delas e como devem fazê-lo. Houve fortes argumentos a favor da consistência e da responsabilização. Defensores cujo trabalho se concentrou especificamente na Internet consideraram os valores da abertura e da confiança como essenciais para o florescimento da Internet e que a tecnologia deve ser confiável e segura para que isso seja alcançado.[175]

Houve também consenso de que existe uma falta de uniformidade ou transparência no que diz respeito à forma como as plataformas lidam com o material de abuso sexual infantil na ausência de regulação. Entrevistados perceberam uma discrepância que deveria ser abordada e identificaram a necessidade de orientações claras às empresas para lhes dizer o que se espera delas e como devem fazê-lo. Houve fortes argumentos a favor da consistência e da responsabilização. Defensores cujo trabalho se concentrou especificamente na Internet consideraram os valores da abertura e da confiança como essenciais para o florescimento da Internet e que a tecnologia deve ser confiável e segura para que isso seja alcançado.[176]

Uma preocupação semelhante que surgiu a partir das entrevistas foi que, onde as plataformas são excessivamente poderosas, isso poderia gerar um enfraquecimento de outros serviços, como os serviços sociais e de educação. Uma atenção excessiva às plataformas levaria a uma preocupação restrita relacionada a soluções tecnológicas e a uma correspondente incapacidade de ter plenamente em conta os papéis que outros serviços desempenham, as suas necessidades e a forma como interagem no ecossistema mais amplo.

Por outro lado, os entrevistados que enfatizaram o foco na tecnologia como natural tenderam a destacar que, em última análise, as ferramentas que as empresas privadas constroem beneficiam a aplicação da lei, uma vez que estão sendo utilizadas para denunciar a exploração e o abuso sexual infantil às autoridades.[177]

174 Entrevista de CRIN e ddm com Richard Wingfield, 6 de setembro de 2022.

175 Estes pontos foram apresentados de forma mais clara na entrevista de CRIN e ddm com a ISOC, 30 de agosto de 2022.

176 Conversa entre CRIN e ddm com representante da sociedade civil, 1 de junho de 2022.

177 WeProtect Global Alliance and ECPAT International, *Technology, privacy and rights: keeping children safe from child sexual exploitation and abuse online - Expert Roundtable Outcomes Briefing*, 8 de abril de 2021, https://www.weprotect.org/wp-content/uploads/Technology-privacy-and-rights-roundtable-outcomes-briefing.pdf



## Para além da Europa e da América do Norte

Para que as leis sejam eficazes, devem ser bem adaptadas aos contextos e estruturas regulatórias nacionais. A mesma lei transplantada de uma jurisdição para outra também pode ter impacto e implementação significativamente diferentes. Tal como um entrevistado expressou: "[a]qui existe o perigo de replicar a legislação de uma jurisdição noutra. É sempre importante ter consultas amplas, públicas e transparentes, a fim de desenvolver legislação adaptada a cada jurisdição."[178]

Um participante destacou que aqueles que trabalham fora da Europa e da América do Norte enfrentam um conjunto específico de desafios ao lidar com a questão da regulação de plataformas.[179] Uma vez que as *big techs* estão majoritariamente baseadas nos EUA e na Europa, a maioria das suas abordagens e recursos são direcionados para essas áreas geográficas.[180] R Pesquisas destacam o fenômeno da "discriminação por *design*", em que algumas crianças têm menos privacidade e menos proteção do que outras na mesma plataforma, dependendo de onde vivem no mundo.[181] Consequentemente, é necessário haver um envolvimento substancialmente maior entre plataformas e países de fora da Europa e da América do Norte, que representam uma elevada proporção do número de usuários, a fim de se levar diversos contextos e especificidades em conta. Por exemplo, as soluções tecnológicas que as plataformas podem adotar para proteger os direitos das crianças online precisam ser compatíveis com a grande variedade de dispositivos que as crianças utilizam em todo o mundo. Crucialmente, isso inclui dispositivos de baixo custo. Outra preocupação diz respeito ao acesso das crianças à Internet. Um exemplo importante aqui é a prática do zero rating, especialmente nos mercados em desenvolvimento: o oferecimento de pacotes que proporcionam acesso gratuito a aplicações e serviços específicos. As plataformas às quais as crianças têm livre acesso controlarão, na prática, o fluxo de informação. O fato de essas plataformas serem encriptadas ou não terá um impacto desproporcional nas crianças se não conseguirem ter acesso a alternativas.

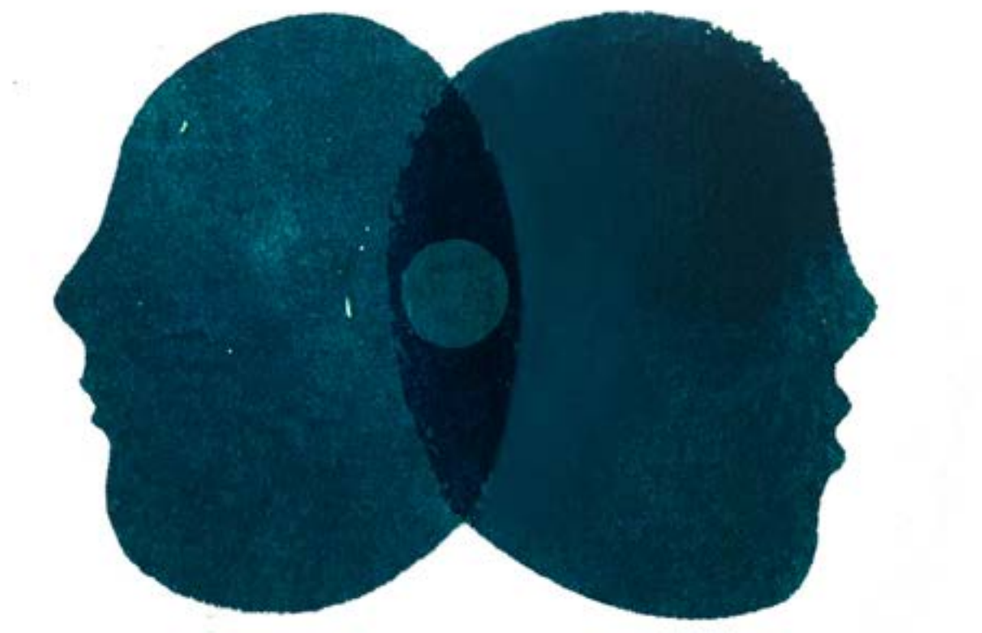
Uma das pessoas entrevistadas argumentou que há uma tensão particular em jogo. Por um lado, os países fora dos espaços anglocêntricos e eurocêntricos precisam fazer mais esforços para implementar regulação que responsabilize as plataformas. Por outro lado, existe um perigo real de que, em jurisdições onde a regulação está menos avançada, as plataformas não estendam as mesmas proteções que oferecem às crianças de países "mais próximos do centro de decisão". Ao mesmo tempo, a regulação é um processo difícil e lento, pelo que, de forma realista, em algumas jurisdições ficará constantemente aquém das iniciativas das plataformas. Nesse caso, as plataformas ainda devem ser pressionadas a tomar medidas proativas na proteção dos direitos das crianças no ambiente digital. Isso poderia ser alcançado, por exemplo, fazendo uso criativo de legislações que não sejam especificamente sobre criptografia, como leis de proteção à criança ou de proteção ao consumidor.

178 Entrevista de CRIN e ddm com um representante da sociedade civil, 12 de agosto de 2022.

179 Estes pontos foram levantados na entrevista de CRIN e ddm com o Instituto Alana, em 22 de setembro de 2022.

180 Um exemplo dado foi a lacuna linguística do Facebook na moderação de conteúdo: WIRED, Facebook Is Everywhere; Sua moderação não está nem perto, 25 de outubro de 2021, https://www.wired.com/story/facebooks-global-reach-exceeds-linguistic-grasp/

181 Fairplay, *Global platforms, partial protections: Design discriminations on social media platforms*, julho 2022, https://fairplayforkids.org/wp-content/uploads/2022/07/design-discriminations.pdf



# O impacto da criptografia nos direitos das crianças

Este capítulo explica o arcabouço dos direitos humanos que se aplica aos direitos das crianças e analisa as implicações da criptografia para esses direitos, com um enfoque especial nas crianças de comunidades desfavorecidas ou marginalizadas.

## O arcabouço internacional dos direitos das crianças

Os direitos humanos - tanto para crianças quanto para adultos - são interdependentes, não hierárquicos e se reforçam mutuamente. Para que tenham efeito, eles devem ser lidos e aplicados juntos e em sua totalidade. Todos os Estados, com exceção dos Estados Unidos, ratificaram a Convenção sobre os Direitos da Criança ("CDC").[182][183] É o tratado de direitos humanos mais ratificado do mundo e, portanto, fornece uma base internacionalmente acordada para o escopo e conteúdo dos direitos das crianças. A CDC reconhece direitos civis e políticos, bem como direitos econômicos, sociais e culturais. A prática e a jurisprudência do Comitê sobre os Direitos da Criança ("o Comitê"), por meio de seus Comentários Gerais, Comunicações e Avaliações Estatais, também fornecem orientações oficiais sobre como a CDC se aplica.

### Princípios gerais

Dentro da CDC, os quatro "princípios gerais" são tanto direitos em si mesmos quanto ferramentas para interpretar e aplicar os outros direitos previstos na Convenção.

Não-discriminação (Art. 2º da CDC)

Os Estados devem garantir que todos os direitos dentro da CDC sejam respeitados para todas as crianças, sem discriminação. As bases da proibição da discriminação estabelecidas na CDC não são exaustivas e, até o momento, o Comitê reconheceu mais de 50 bases de discriminação proibida. Como o Comitê explicou, esse direito exige que as crianças tenham acesso igualitário e efetivo ao ambiente digital e que elas não sejam discriminadas, seja pela exclusão do uso de tecnologias e serviços digitais, pelo recebimento de comunicações de ódio ou pelo tratamento injusto por meio dessas tecnologias.[184]

182 Convenção sobre os Direitos da Criança, disponível em: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

183 N.T.: recomendamos a versão em português da Convenção sobre os Direitos da Criança traduzida pela UNICEF: https://www.unicef.org/brazil/convencao-sobre-os-direitos-da-crianca

184 Comitê dos Direitos da Criança da ONU, Comentário Geral No. 25 (2021) sobre os direitos da criança em relação ao ambiente digital, CRC/C/GC/25, 2 de março de 2021, § 9-11.

Melhor interesse da criança (Art. 3º da CDC)

Em todas as ações que envolvem crianças, seu melhor interesse deve ser uma consideração primordial. Esse direito tem três aspectos:[185]

1. Um direito substantivo: ao tomar decisões que afetam crianças, os Estados devem alcançar um resultado que trate os melhores interesses das crianças como uma consideração primordial.
2. Um direito procedimental: sempre que uma decisão que afetará uma criança, um grupo de crianças ou crianças em geral for tomada, o processo deve incluir uma avaliação do impacto da decisão nas crianças.
3. Um direito interpretativo: se uma disposição legal permitir mais de uma interpretação, a interpretação que melhor serve aos melhores interesses da criança deve ser escolhida.

Qualquer consideração sobre o que está de acordo com os melhores interesses da criança deve incluir o respeito pelo direito das crianças de serem ouvidas, e as opiniões das crianças devem ser consideradas com o devido peso.

Direito à vida, sobrevivência e desenvolvimento (Art. 6º da CDC)

Todas as crianças têm o direito à vida e os Estados são obrigados a garantir, na medida do possível, a sobrevivência e o desenvolvimento da criança. Em relação ao ambiente digital, o Comitê destacou especificamente que os riscos "relacionados a conteúdo, contato, conduta e contrato, abrangem, entre outras coisas, conteúdo violento e sexual, ciberagressão e assédio, jogos de azar, exploração e abuso, incluindo exploração e abuso sexual, e a promoção ou incitação ao suicídio ou atividades que ameacem a vida, inclusive por parte de criminosos ou grupos armados considerados como terroristas ou extremistas violentos."[186]

Direito de ser ouvido (Art. 12 da CDC)

As crianças têm o direito de expressar suas opiniões livremente em todos os assuntos que as afetam e que suas opiniões sejam consideradas com o devido peso, de acordo com sua idade e maturidade. Isso não é apenas um direito processual que exige que tenham a oportunidade de expressar suas opiniões, mas também exige que os Estados ajam com base nessas opiniões. O direito se aplica não apenas a decisões que afetam uma criança individualmente, mas também àquelas que afetam as crianças como grupo.[187] O Comitê recomendou aos Estados que "deveriam envolver todas as crianças, ouvir suas necessidades e dar o devido peso às suas opiniões. Eles devem garantir que os provedores de serviços digitais se envolvam ativamente com as crianças, aplicando salvaguardas apropriadas e dando devida consideração às opiniões delas ao desenvolver produtos e serviços."[188]

## Outros direitos fundamentais no contexto da criptografia

Capacidades em evolução (Art. 5º da CDC)

Embora não seja em si um princípio geral da CDC, o conceito de "capacidades em evolução" desempenha um papel importante na realização e aplicação dos direitos das crianças. Refere-se à responsabilidade dos pais (e outros) de "ajustar continuamente os níveis de apoio e orientação oferecidos a uma criança", dependendo dos "interesses e desejos da criança", bem como de suas "capacidades para a tomada de decisões autônomas" e compreensão de seus melhores interesses.[189]

Violência contra crianças (Arts. 19, 34, 39 da CDC)

Os Estados são obrigados a adotar todas as medidas legislativas, administrativas, sociais e educacionais adequadas para proteger as crianças de todas as formas de violência, incluindo violência física, mental e sexual. Essas medidas de proteção devem incluir programas sociais para fornecer apoio às crianças e àqueles que cuidam delas, bem como outras medidas para prevenção, identificação, denúncia, encaminhamento, investigação, tratamento e acompanhamento de casos de maus tratos. Os Estados também são obrigados a adotar todas as medidas adequadas para promover a recuperação física e psicológica das crianças vítimas de violência.

Liberdade de expressão (Art. 13 da CDC)

As crianças têm o direito à liberdade de expressão, incluindo a liberdade de buscar, receber e transmitir informações e ideias de todos os tipos. Esse direito pode ser sujeito a restrições estabelecidas por lei e necessárias para o respeito aos direitos ou à reputação de outras pessoas e para a proteção da segurança nacional, da ordem pública ou da saúde ou moral públicas. Aplicando esse direito, o Comitê afirmou que "[q]uaisquer restrições ao direito das crianças à liberdade de expressão no ambiente digital, como filtros, incluindo medidas de segurança, devem ser legais, necessários e proporcionais. A justificativa para tais restrições deve ser transparente e comunicada às crianças de maneira ade-

185 Veja: Comitê dos Direitos da Criança da ONU, Comentário Geral No. 14 (2013) sobre o direito da criança de ter seu melhor interesse tomado como consideração primária, CRC/C/GC/14, 29 de maio de 2013, § 6, disponível em: https://www2.ohchr.org/english/bodies/crc/docs/gc/crc_c_gc_14_eng.pdf

186 Comitê dos Direitos da Criança da ONU, Comentário Geral No. 25 (2021) sobre os direitos da criança em relação ao ambiente digital, CRC/C/GC/25, 2 de março de 2021, § 14.

187 Veja, por exemplo, Comitê dos Direitos da Criança da ONU, Comentário Geral No. 12 (2009) - O direito da criança de ser ouvida, CRC/C/GC/12, https://www2.ohchr.org/english/bodies/crc/docs/advanceversions/crc-c-gc-12.pdf

188 Comitê dos Direitos da Criança da ONU, Comentário Geral No. 25 (2021) sobre os direitos da criança em relação ao ambiente digital, CRC/C/GC/25, 2 de março de 2021, ª 17.

189 Veja, por exemplo, Comitê dos Direitos da Criança da ONU, Comentário Geral No. 7 (2005) - Implementando direitos das crianças na primeira infância, CRC/C/GC/7/Rev.1, 20 de setembro de 2006, § 17, https://www2.ohchr.org/english/bodies/crc/docs/AdvanceVersions/GeneralComment7Rev1.pdf

quada à sua idade."[190] O Comitê também recomendou que os Estados protejam as crianças contra agressões cibernéticas, ameaças, censura, violações de dados e vigilância digital.[191]

Acesso à informação (Arts. 13, 17 da CDC)

Além do reconhecimento do direito das crianças de buscar e receber informações e ideias de todos os tipos, a CDC exige que os Estados garantam que as crianças tenham acesso a informações e materiais de diversas fontes nacionais e internacionais, especialmente aqueles voltados para a promoção do bem estar social, espiritual e moral, bem como da saúde física e mental. O Comitê recomendou que os Estados garantam que os provedores de serviços digitais cumpram as diretrizes, normas e códigos relevantes e apliquem regras de moderação de conteúdo legais, necessárias e proporcionais, mas que a moderação de conteúdo e os controles sejam equilibrados com o direito à proteção dos outros direitos das crianças, incluindo os direitos à liberdade de expressão e privacidade.[192]

Liberdade de associação e reunião pacífica (Art. 15 da CDC)

As crianças têm o direito à liberdade de associação e reunião pacífica. Esse direito não deve ser restringido, exceto em conformidade com a lei e necessário em uma sociedade democrática, no interesse da segurança nacional ou da segurança pública, da ordem pública, da proteção da saúde ou públicas, ou da proteção dos direitos e liberdades de outrem. O Comitê reconheceu que "[a] visibilidade pública e as oportunidades de estabelecer redes e conexões no ambiente digital também podem apoiar o ativismo liderado por crianças e capacitar as crianças como defensoras dos direitos humanos", e que "o ambiente digital permite que as crianças, incluindo as defensoras de direitos humanos, bem como as crianças em situações vulneráveis, se comuniquem entre si, advoguem por seus direitos e formem associações."[193]

Direito à privacidade (Art. 16 da CDC)

Nenhuma criança deve ser sujeita a interferência arbitrária ou ilegal em sua privacidade, família, lar ou correspondência, nem a ataques ilegais à sua honra e reputação. As crianças têm o direito à proteção da lei contra tais interferências ou ataques. O Comitê reconheceu que a privacidade é vital para a autonomia, dignidade e segurança das crianças e para o exercício de seus direitos.[194]

190 Comitê dos Direitos da Criança da ONU, Comentário Geral No. 25 (2021) sobre os direitos da criança em relação ao ambiente digital, CRC/C/GC/25, 2 de março de 2021, § 59.

191 Ibidem.

192 Idem, § 56.

193 Idem, § 66.

194 Idem, § 67.



Direito ao mais alto padrão alcançável de saúde (Art. 24 da CDC)

As crianças têm direito ao mais alto padrão alcançável de saúde. No contexto do ambiente digital, o Comitê reconheceu o desejo das crianças de "acesso a serviços de saúde mental e de saúde sexual e reprodutiva *online* gratuitos, confidenciais, adequados à idade e não discriminatórios" e recomendou que os Estados "garantam que as crianças tenham acesso seguro, confidencial e confiável a informações e serviços de saúde confiáveis, incluindo serviços de aconselhamento psicológico." O Comitê também recomendou que "[t]ais serviços devem limitar o processamento dos dados das crianças ao estritamente necessário para a prestação do serviço e devem ser fornecidos por profissionais ou pessoas com treinamento adequado, com mecanismos regulados de supervisão em vigor."[195]

Acesso à justiça

O Comitê reconheceu que as crianças enfrentam desafios específicos na aplicação de seus direitos relacionados ao ambiente digital, por exemplo, devido à falta de legislação específica, às dificuldades em identificar os infratores ou à falta de conhecimento de seus direitos. Portanto, o Comitê afirmou que os Estados devem garantir que remédios apropriados e eficazes estejam disponíveis para violações aos direitos das crianças, inclusive no ambiente digital. Os Estados devem fornecer mecanismos de reclamação e denúncia que sejam gratuitos, seguros, confidenciais, responsivos, adequados às crianças e acessíveis. Eles também devem estabelecer estruturas para o encaminhamento de casos e fornecer apoio eficaz às crianças que são vítimas. Em particular, eles devem fornecer treinamento especializado para autoridades policiais, promotores e juízes. Os Estados também devem garantir que as empresas forneçam mecanismos eficazes de reclamação, e que as agências com poderes de supervisão legal relevantes para os direitos das crianças investiguem reclamações e forneçam remédios adequados para violações dos direitos das crianças.[196]

A tabela abaixo apresenta uma análise de como a gama completa dos direitos das crianças é afetada pela criptografia, seja de forma positiva ou negativa.

195 Idem, § 94.

196 Idem, § 43-49.

| O direito | Os benefícios da criptografia | Os riscos da criptografia |
|---|---|---|
| **Não-discriminação** (Art. 2º da CDC) | • A criptografia protege a comunicação de todas as crianças, incluindo aquelas que não estão cientes dos benefícios da criptografia.<br>• Ela oferece benefícios específicos para crianças de grupos desfavorecidos ou marginalizados, que enfrentam mais riscos *online* com base no que comunicam, como crianças LGBT+, crianças indígenas, crianças de grupos étnicos ou religiosos minoritários, crianças afetadas pela violência doméstica, crianças envolvidas em ativismo político em contextos onde isso representa um risco, e crianças com deficiências.<br>• A criptografia protege mulheres e meninas contra a divulgação involuntária de informações, já que enfrentam ameaças específicas de vigilância, assédio e violência *online*. | • Conteúdo que promove a discriminação, seja de forma geral ou contra crianças específicas, pode circular sem ser detectado em plataformas criptografadas.<br>• Se as autoridades policiais não tiverem acesso às comunicações porque estão criptografadas, elas podem usar outros dados (como metadados ou sinais de comportamento) de maneira discriminatória. |
| **Direito à vida** (Art. 6º da CDC) | Plataformas criptografadas mantêm as comunicações privadas, garantindo a segurança daqueles que, de outra forma, seriam alvos de situações que colocam suas vidas em risco com base no conteúdo de suas comunicações. | • Plataformas criptografadas facilitam o compartilhamento, de forma não detectada, de comunicações que ameaçam a vida de crianças (por exemplo, incitação ao suicídio, discurso de ódio e incitação à violência que poderiam resultar em mortes, o planejamento de ataques terroristas ou outros crimes).<br>• Crianças que foram vítimas de abuso sexual perpetrado por meio de canais criptografados podem tentar se ferir ou tirar suas próprias vidas.. |
| **Direito a ser ouvido. Liberdade de expressão e de informação** (Arts. 12, 13 da CDC) | • A privacidade proporcionada pela criptografia fortalece a liberdade de expressão e informação das crianças. Isso lhes oferece a oportunidade de expressar suas opiniões e buscar, receber e compartilhar informações sobre uma variedade de tópicos, incluindo questões políticas, sociais, culturais e religiosas, sem medo de retaliações. Isso se aplica especialmente para crianças de grupos desfavorecidos ou marginalizados. | • A disseminação de "informações ruins", como desinformação ou discurso de ódio, por meio de canais criptografados pode levar as crianças à autocensura ao buscar informações.<br>• As crianças não podem acessar informações criptografadas de interesse para elas ou para o público em geral sem a chave. |
| **Liberdade de pensamento, consciência e religião** (Art. 14 da CDC) | • Minorias religiosas podem usar canais criptografados para se comunicarem de forma segura.<br>• Ao proteger a privacidade de suas comunicações, a criptografia pode manter a liberdade de pensamento daqueles cujas crenças podem não ser amplamente aceitas na sociedade (por exemplo, defensores dos direitos ao aborto).<br>• As próprias plataformas não podem monitorar o conteúdo das comunicações criptografadas de ponta a ponta, portanto, elas não têm dados que lhes permitam "manipular ou interferir no direito das crianças à liberdade de pensamento e crença no ambiente digital, por exemplo, por meio de análises emocionais ou inferências".[197] | • Canais criptografados podem ser usados para propagar discurso de ódio contra minorias religiosas ou circular informações que ameacem a liberdade de pensamento das crianças.[198] |

197 Comitê dos Direitos da Criança da ONU, Comentário Geral No. 25 (2021) sobre os direitos da criança em relação ao ambiente digital, CRC/C/GC/25, 2 de março de 2021, § 62.

198 O impacto da tecnologia na liberdade de pensamento é uma questão subexplorada, particularmente no tocante à manipulação das emoções dos usuários. Em 2017, foi apontado que o Facebook mostrava para os anunciantes como identificar dados emocionais de seus usuários jovens: The Guardian, Facebook told advertisers it can identify teens feeling 'insecure' and 'worthless', 1 de Maio de 2017, https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens. Anteriormente, a companhia publicou os resultados de um experimento no qual tinha manipulado a informação postada no feed de notícias de 689.003 usuários e tinha descoberto que as emoções das pessoas era reforçada pelo que elas viam, num processo de "contágio emocional": The Guardian, Facebook emotion study breached ethical guidelines, researchers say, 30 de junho de 2014, https://www.theguardian.com/technology/2014/jun/30/facebook-emotion-study-breached-ethical-guidelines-researchers-say

| | | |
|---|---|---|
| **Liberdade de associação e liberdade de reunião pacífica** (Art. 15 da CDC) | • A criptografia pode permitir que jovens manifestantes se organizem sem medo de serem alvos de represálias. | • Plataformas criptografadas podem ser usadas para propagar discurso de ódio sobre crianças específicas ou grupos de crianças (especialmente aquelas desfavorecidas ou marginalizadas), o que poderia fazer com que elas tenham medo de exercer suas liberdades de associação e reunião pacífica. |
| **Privacidade** (Art. 16 da CDC) | • Ao limitar o número de pessoas que podem ver as informações que as crianças trocam online ou acessar seus dados, a criptografia beneficia a privacidade das crianças. Saber que não estão sendo continuamente vigiadas, seja *online* ou *offline*, ajuda as crianças a desenvolverem confiança em seus pais, professores ou outras pessoas com quem têm relacionamentos pessoais, tornando mais provável que peçam ajuda quando precisam.<br>• Privacidade e construção de confiança são particularmente importantes para crianças que têm um maior risco de serem alvo pelo que comunicam, especialmente aquelas de comunidades desfavorecidas ou marginalizadas. | • Serviços criptografados podem ser usados para disseminar conteúdo que viola a privacidade das crianças, como informações não consensuais e material de abuso sexual infantil. |
| **Proteção contra informações e materiais prejudiciais ao bem estar** (Art. 17(e) da CDC) | • Existe o perigo de que a linguagem de proteção do Artigo 17 da CDC seja usada de forma inadequada para justificar proibições de certos tipos de informações destinadas a crianças (por exemplo, a proibição de "propaganda gay" na Rússia e em alguns países da Europa Oriental e Ásia Central) ou que seja mal aplicada para promover preconceito entre crianças (por exemplo, por meio de propaganda racista). Quando isso acontece, aqueles que se organizam contra o uso inadequado da linguagem de proteção podem utilizar canais criptografados para evitar serem alvo. | • Canais criptografados podem ser usados para disseminar informações prejudiciais ao bem estar das crianças, como material de abuso sexual infantil ou discursos de ódio. Eles dificultam a identificação e remoção desse conteúdo e a identificação dos responsáveis. |



| | | |
|---|---|---|
| **Proteção contra violência e exploração** (Art. 19 da CDC) | • • Serviços criptografados podem proteger as crianças de serem alvos de violência com base nas informações que enviam ou recebem, especialmente quando fazem parte de grupos desfavorecidos ou marginalizados.<br>• O acesso aos dados pessoais das crianças pode torná-las vulneráveis ao assédio e à exploração, mas a criptografia ajuda a manter os dados seguros.<br>• Crianças que são exploradas sexualmente podem se comunicar de forma segura por meio de canais criptografados para pedir ajuda, armazenar ou enviar evidências, etc. | • A criptografia pode facilitar a violência contra crianças, especialmente o abuso sexual, permitindo, por exemplo, que os perpetradores acessem e disseminem material de abuso sexual infantil *online* sem serem detectados.<br>• A criptografia mantém as comunicações entre a criança e o perpetrador privadas no caso de assédio, *bullying* ou perseguição, tornando mais difícil investigar e processar o abuso. |
| **Saúde e serviços de saúde** (Art. 24 da CDC) | • • Os dados dos pacientes podem ser compartilhados e armazenados de forma segura graças à criptografia.<br>• Plataformas criptografadas facilitam o compartilhamento de informações sobre saúde, especialmente quando elas podem ser censuradas de outra forma (por exemplo, pais compartilhando fotos da condição de saúde de seus filhosferramentas automatizadas podem bloqueá-las; informações sobre prevenção e tratamento do HIV compartilhadas por grupos LGBT+). | • A desinformação sobre saúde pode circular em canais criptografados sem ser detectada.<br>• Plataformas criptografadas podem ser usadas para disseminar informações que ameacem a saúde das crianças, como transtornos alimentares ou automutilação.<br>• Plataformas criptografadas podem ser usadas para facilitar a violência contra crianças, colocando em risco sua saúde física e mental. |
| **Padrão de vida adequado** (Art. da 27 CDC) | • Criptografia facilita transações financeiras seguras. | |
| **Direito à educação** (Art. da 28 CDC) | • Canais criptografados podem ser usados para compartilhar informações educacionais e orientações vocacionais que, de outra forma, seriam censuradas. | |

| | | |
|---|---|---|
| **Direito ao lazer, brincadeira e cultura** (Art. 31 da CDC) | • Plataformas criptografadas podem ser usadas para compartilhar informações que facilitam a participação das crianças em atividades culturais, artísticas, recreativas e de lazer em contextos onde essa informação de outra forma poderia ser censurada. | |
| **Exploração sexual** (Art. 34 da CDC) | • O acesso aos dados pessoais das crianças pode torná-las vulneráveis ao assédio e à exploração, mas a criptografia ajuda a manter os dados seguros.<br>• Crianças que são exploradas sexualmente podem se comunicar de forma segura por meio de canais criptografados para pedir ajuda, armazenar ou enviar evidências, etc. | • A criptografia pode facilitar a exploração sexual e o abuso de crianças, permitindo, por exemplo, que os perpetradores se comuniquem entre si ou acessem e disseminem material de abuso sexual infantil online sem serem detectados.<br>• A criptografia mantém as comunicações entre a criança e o perpetrador privadas no caso de assédio, tornando mais difícil investigar e processar o abuso. |
| **Sequestro, venda e tráfico** (Art. 35 da CDC) | • Crianças vítimas de tráfico podem se comunicar de forma segura por meio de canais criptografados para pedir ajuda, armazenar ou enviar evidências. | • Plataformas criptografadas podem ser usadas por traficantes de crianças para facilitar o sequestro, venda e tráfico de crianças. |
| **Proteção de crianças afetadas por conflito armado** (Art. 38 da CDC) | • Durante conflitos armados, as mensagens criptografadas garantem comunicações seguras entre civis, incluindo crianças. | • Durante conflitos armados, canais criptografados podem ser usados para planejar atividades que ameaçam o direito à proteção de civis, incluindo crianças. |
| **Justiça juvenil** (Art. 40 CRC) | • O armazenamento e a transferência de dados criptografados, por exemplo, em casos judiciais envolvendo crianças, podem facilitar a administração tranquila e segura da justiça juvenil.<br>• Ao usar a criptografia, as autoridades policiais podem evitar vazamentos de materiais de investigação. | |



## Privacidade: seu escopo, a ligação com a proteção e restrições permitidas

O direito à privacidade - tanto para crianças quanto para adultos - tem desempenhado um papel central no debate sobre a regulação da criptografia. No entanto, uma análise mais detalhada do direito à privacidade e de suas restrições permitidas pode estabelecer um quadro para lidar com tal regulação de maneira respeitosa aos direitos das crianças, mesmo quando houver tensões na aplicação dos direitos das crianças de forma mais ampla.

### *Escopo*

O direito à privacidade das crianças está bem estabelecido no direito internacional dos direitos humanos. Ele está consagrado em vários tratados e declarações,[199] incluindo, como visto acima, na Convenção sobre os Direitos da Criança (CDC), que proíbe a interferência arbitrária ou ilegal na privacidade ou na correspondência das crianças.[200] A proteção do direito à privacidade sob a CDC é idêntica à do Pacto Internacional de Direitos Civis e Políticos, com a exceção da adição da palavra "criança", o que indica uma proteção equivalente para a privacidade das crianças em relação à dos adultos.

O direito à privacidade desempenha um papel importante no desenvolvimento das crianças. O Comitê afirmou que "a privacidade é vital para a agência [e] dignidade das crianças"[201] O direito ao respeito pela vida privada e familiar, sob a Convenção Europeia de Direitos Humanos, por exemplo, foi interpretado como protegendo "o direito ao desenvolvimento pessoal, seja em termos de personalidade ou de autonomia pessoal".[202] Ele também inclui "o direito de cada indivíduo de se aproximar de outros para estabelecer e desenvolver relacionamentos com eles e com o mundo exterior, ou seja, o direito a uma 'vida social privada'".[203]

### *Privacidade e proteção*

Como o Comitê reconheceu, a privacidade possibilita o "exercício dos [direitos das crianças]". Às vezes referido como um direito "facilitador" ou "porta de entrada",[204]

199 Por exemplo, Art. 17 do Pacto Internacional sobre Direitos Civis e Políticos, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights; Art.12 da Declaração Universal dos Direitos Humano, https://www.un.org/en/about-us/universal-declaration-of-human-rights

200 Art. 16 da Convenção sobre os Direitos da Criança.

201 Comitê dos Direitos da Criança da ONU, Comentário Geral No. 25 (2021) sobre os direitos da criança em relação ao ambiente digital, CRC/C/GC/25, 2 de março de 2021, § 67

202 *Bărbulescu v. Romania [Tribunal Europeu dos Direitos Humanos, Grande Câmara], App. No. 61496/08, 5 de setembro de 2017, § 70.*

203 Idem, § 70-71. Veja também: Tribunal Europeu dos Direitos Humanos (Registro), Guia sobre o Artigo 8 da Convenção Europeia de Direitos Humanos, Respeito pela vida privada e familiar, atualizado em 31 de agosto de 2022.

204 Lorna McGregor, First Report of the UN Special Rapporteur on the Right to Privacy to the Human Rights Council, EJIL: Talk!, 18 de março de 2016, https://www.ejiltalk.org/first-report-of-the-un-special-rapporteur-on-the-right-to-privacy-to-the-human-rights-council/

a privacidade facilita o gozo de outros direitos, incluindo a liberdade de expressão e informação, liberdade de associação, liberdade de pensamento, consciência e religião, direito à saúde e não discriminação.

O Comitê também reconheceu que a privacidade é vital para a dignidade, segurança e o exercício dos direitos das crianças.[205]Portanto, o Comitê reconheceu que a privacidade não se opõe à proteção das crianças contra a violência - pelo contrário, a privacidade tem um elemento de proteção. Na verdade, violações do direito à privacidade podem ter consequências muito sérias, incluindo danos físicos ou psicológicos. Isso é particularmente verdadeiro para crianças de grupos desfavorecidos e marginalizados, como discutido abaixo.

### *Restrições*

O direito à privacidade é qualificado, não absoluto, e, portanto, pode ser restringido em certas circunstâncias.

Como o Comitê explicou, isso significa que qualquer interferência na privacidade das crianças deve ser "prevista por lei, destinada a servir a um propósito legítimo, manter o princípio da minimização de dados, ser proporcional e projetada para observar o melhor interesse da criança e não deve conflitar com as disposições, metas ou objetivos da Convenção".[206] Segundo o Comitê de Direitos Humanos das Nações Unidas, as restrições à privacidade não podem "prejudicar a essência" do direito.[207]

No que diz respeito especificamente à criptografia, o Comitê dos Direitos da Criança afirmou que, "[q]uando a criptografia é considerada um meio apropriado, os Estados-membros devem considerar medidas apropriadas que permitam a detecção e a denúncia de exploração sexual e abuso sexual infantil ou material de abuso sexual infantil".[208] Ele reafirmou os limites das limitações admissíveis sob o direito internacional dos direitos humanos, acrescentando que as medidas "devem ser estritamente limitadas de acordo com os princípios de legalidade, necessidade e proporcionalidade".[209]

O Comitê sugeriu que medidas rotineiras e indiscriminadas não são necessárias nem proporcionais. Por exemplo, o Comitê destacou que práticas como o processamento automatizado de dados, a verificação obrigatória de identidade, a filtragem de informações e a vigilância em massa estão "se tornando rotineiras" e "podem levar a interferências arbitrárias ou ilegais na privacidade das crianças", o que poderia continuar a afetá-las posteriormente em suas vidas.[210] Nesse sentido, o Comitê afirmou que a vigilância digital e o processamento automatizado de dados associados devem respeitar a privacidade das crianças e "não devem ser realizados rotineira ou indiscriminadamente" ou sem o conhecimento da criança. Ele também enfatizou que "sempre deve ser dada consideração aos meios menos intrusivos à privacidade disponíveis para cumprir o propósito desejado".[211]

O Alto Comissariado das Nações Unidas para os Direitos Humanos usou linguagem semelhante, alertando que um "impacto generalizado e indiscriminado [no direito à privacidade] não é compatível com o princípio da proporcionalidade".[212] O Comissariado observou que "a maioria das restrições à criptografia [na privacidade e nos direitos associados] é desproporcional, afetando muitas vezes não apenas os indivíduos visados, mas também a população em geral".[213] O Comissariado, então, alertou contra "todas as restrições diretas ou indiretas, gerais e indiscriminadas" ao uso da criptografia.[214]

Tribunais regionais também usaram linguagem comparável em julgamentos. Em relação a pessoas suspeitas, mas não condenadas por crimes, o Tribunal Europeu de Direitos Humanos, por exemplo, considerou que "a natureza geral e indiscriminada" da retenção de impressões digitais e DNA não representava "um justo equilíbrio entre os interesses públicos e privados em conflito" e, portanto, não era uma interferência necessária e proporcional no direito ao respeito pela vida privada.[215] Em relação a dados de tráfego e localização, o Tribunal de Justiça da União Europeia considerou que a única instância em que "a retenção geral e indiscriminada" e "a análise automatizada" desses dados podem ser proporcionais é quando a duração da retenção for estritamente necessária para responder a uma ameaça séria, genuína, presente ou previsível para a segurança nacional.[216] Em relação ao conteúdo das comunicações eletrônicas, o Tribunal usou até mesmo uma linguagem mais forte, indicando que leis que permitem às autoridades públicas "acesso generalizado" a dados de conteúdo comprometem a essência do direito ao respeito pela vida privada.[217]

---

205 Comitê dos Direitos da Criança da ONU, Comentário Geral No. 25 (2021) sobre os direitos da criança em relação ao ambiente digital, CRC/C/GC/25, 2 de março de 2021, § 67.

206 Idem, § 69.

207 Comitê dos Direitos Humanos ONU, Comentário Geral No. 31 (2004): A natureza da obrigação jurídica geral imposta aos Estados Partes no Pacto, 26 de maio de 2004, § 6, https://www.refworld.org/docid/478b26ae2.html; Alto Comissariado das Nações Unidas para os Direitos Humanos, O direito à privacidade na era Digital, A/ HRC/51/17, 4 de agosto de 2022, § 56.

208 Comitê dos Direitos da Criança da ONU, Comentário Geral No. 25 (2021) sobre os direitos da criança em relação ao ambiente digital, CRC/C/GC/25, 2 de março de 2021, § 70.

209 Ibidem.

210 Idem, § 68.

211 Idem, § 75.

212 Alto Comissariado das Nações Unidas para os Direitos Humanos, O direito à privacidade na era Digital, A/HRC/39/29, 3 de agosto de 2018, § 20.

213 Alto Comissariado das Nações Unidas para os Direitos Humanos, O direito à privacidade na era Digital, A/HRC/51/17, 4 de Agosto de 2022, § 25.

214 Idem, § 57 (b)

215 *S. e Marper versus Reino Unido [Tribunal Europeu de Direitos Humanos], App. Nos. 30562/04 e 30566/04, 4 de dezembro de 2008, § 125.*.

216 *La Quadrature du Net e Outros v. Primeiro ministro e Outros [Tribunal de Justiça da União Europeia, Grande Câmara], Casos reunidos C-511/18, C-512/18 e C-520/18, 6 de Outubro de 2020, § 177.*.

217 *Maximillan Schrems v. Comissário para a Proteção de Dados [Tribunal de Justiça da União Europeia, Grande Secção], Case C-362/14, 6 de outubro de 2015, § 94.*.

## O papel das empresas

Empresas privadas desempenham um papel crucial no debate sobre criptografia e direitos das crianças devido ao seu papel central no ambiente digital. Embora a Convenção estabeleça as obrigações dos Estados em relação aos direitos das crianças, o Comitê reconheceu que os deveres e responsabilidades de respeitar esses direitos também se estendem na prática às empresas.[218]

O Comitê reconheceu a relevância do *framework "Protect, Respect and Remedy"* [Proteger, Respeitar e Reparar] das Nações Unidas (PRR) e dos Princípios Orientadores sobre Empresas e Direitos Humanos,[219] bem como dos Princípios dos Direitos da Criança e Empresas. O Framework PRR[220] estabelece três princípios: (1) o dever do Estado de proteger contra violações de direitos humanos cometidas por terceiros, incluindo empresas; (2) a responsabilidade corporativa de respeitar os direitos humanos; e (3) a necessidade de um acesso mais eficaz a remédios. Os Princípios Orientadores das Nações Unidas sobre Empresas e Direitos Humanos[221] são um conjunto de princípios para ajudar Estados e empresas a implementar o framework PRR. No que diz respeito às empresas, os princípios se baseiam em dois elementos: um compromisso político de respeitar os direitos humanos e um processo de devida diligência em direitos humanos. Os Princípios dos Direitos da Criança e Empresas[222] estabelecem ações empresariais para respeitar e apoiar os direitos das crianças. O Comitê afirmou que "todas as empresas devem cumprir suas responsabilidades em relação aos direitos das crianças, e os Estados devem garantir que o façam".[223]

No que diz respeito ao ambiente digital especificamente, o Comitê afirmou que "as empresas devem respeitar os direitos das crianças e prevenir e remediar abusos de seus direitos no ambiente digital", enquanto os Estados "têm a obrigação de garantir que as empresas cumpram essas responsabilidades".[224] O Comitê reconheceu que "embora as empresas possam não estar diretamente envolvidas na prática de atos danosos, elas podem causar ou contribuir para violações do direito das crianças a estarem livres de violência, inclusive por meio do design e operação de serviços digitais". Também afirmou que "[os Estados] devem exigir [das empresas] a implementação de estruturas regulatórias, códigos setoriais e termos de serviço que estejam em aderência aos mais altos padrões de ética, privacidade e segurança em relação ao design, engenharia, desenvolvimento, operação, distribuição e marketing de seus produtos e serviços".[225]

218 UN Committee on the Rights of the Child, *General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights*, CRC/C/GC/16, 17 April 2013, para. 8, https://www2.ohchr.org/english/bodies/crc/docs/CRC.C.GC.16.pdf

219 Idem, § 7

220 Disponível em: https://www2.ohchr.org/english/bodies/hrcouncil/docs/8session/a-hrc-8-5.doc

221 Disponível em: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

222 Disponível em: https://www.unicef.org/media/96136/file/Childrens-Rights-Business-Principles-2012.pdf

223 Comitê dos Direitos da Criança da ONU, Comentário Geral No. 16 (2013) sobre as obrigações do Estado a respeito do impacto do setor empresarial nos direitos das crianças, CRC/C/GC/16, 17 de abril de 2013, § 8.

224 Comitê dos Direitos da Criança da ONU, Comentário Geral No. 25 (2021) sobre os direitos da criança em relação ao ambiente digital, CRC/C/GC/25, 2 de Março de 2021, § 35.

225 Idem, § 39.



# Além do paradigma "privacidade versus proteção": alguns cenários

*"Não existe uma visão única e monolítica do que significa ser criança. "*[226]

A gama completa de direitos das crianças integra o debate sobre criptografia, e vai além de qualquer análise construída exclusivamente com base na privacidade versus proteção. Os cenários a seguir exploram várias maneiras pelas quais a criptografia afeta os direitos das crianças, especialmente quando essas crianças pertencem a grupos desfavorecidos ou marginalizados. Esta seção não tem como objetivo fornecer uma discussão exaustiva das maneiras pelas quais a criptografia pode ser relevante para eles. Em vez disso, procura apresentar situações que dão uma ideia da amplitude e complexidade das questões éticas, legais e práticas em jogo. Esses cenários têm como objetivo ampliar a discussão além do paradigma da criptografia como uma questão de privacidade ou proteção. O objetivo é destacar a agência das crianças - sua capacidade de tomar decisões e exercer seus direitos em uma variedade de ambientes públicos e privados, e em relação a outras partes, como o Estado, sua família e comunidade, e, é claro, empresas como plataformas de redes sociais.

## Criptografia, crianças e o Estado

### *Crianças que vivem em regimes repressivos, delatores e ativistas*

Em relação ao Estado, a criptografia desempenha um papel crucial na segurança das comunicações de crianças que seriam alvos e sujeitas à violência pelo governo se o conteúdo de suas buscas ou trocas fosse revelado. Isso vale especialmente para crianças que desejam exercer seus direitos civis e políticos em regimes repressivos, como mostra o primeiro cenário.

**Cenário 1**

Mahsa tem 16 anos e vive em um país conhecido pelos excessos violentos de sua polícia de moralidade. Ela usa plataformas de rede social não criptografadas para organizar um protesto pacífico da juventude contra a brutalidade policial. O governo está monitorando as comunicações nessas plataformas, descobre o protesto e o dispersa à força. A polícia e os serviços de segurança usam dados monitorados em plataformas não criptografadas para identificar pessoas que compareceram ou estiveram envolvidas no planejamento do protesto. Mahsa e outras crianças são presas, espancadas severamente e processadas.

226 Conversa de CRIN e ddm com Associação Data Privacy Brasil de Pesquisa, 24 de novembro de 2022.

Embora este cenário seja inspirado nos protestos iranianos de 2022, nos quais crianças foram intimidadas, presas e mortas,[227] irestrições não permitidas à liberdade de reunião das crianças têm sido documentadas há muito tempo. Após a Primavera Árabe, crianças que protestaram no Egito foram presas, torturadas e assassinadas.[228] No Bahrein, foram espancadas e ameaçadas de estupro e choques elétricos.[229] Na Indonésia, manifestantes infantis foram presos[230] e, na Tailândia, foram alvejados.[231]Em Mianmar, eles enfrentaram repressão brutal.[232]Intimidações foram relatadas até em países com proteção geralmente forte aos direitos políticos e liberdades civis[233] - no Reino Unido, por exemplo, a polícia foi acusada de empregar táticas destinadas a dissuadir crianças de protestar contra as mudanças climáticas.[234]

Esses exemplos mostram que as crianças podem estar em sério risco de sofrer violência física por parte do Estado se não tiverem meios de se comunicar de forma segura para exercer seus direitos. Nesses casos, a privacidade proporcionada pela criptografia também serve ao direito das crianças à proteção contra a violência.

A criptografia também traz benefícios desproporcionais para crianças que podem não estar diretamente em risco de violência física, mas cujos direitos são ameaçados por regimes que praticam vigilância e censura.

227 Human Rights Watch, *In Iran, Schoolgirls Leading Protests for Freedom*, 12 de outubro de 2022, https://www.hrw.org/news/2022/10/12/iran-schoolgirls-leading-protests-freedom

228 The Nation, *The Children of the Arab Spring Are Being Jailed and Tortured*, 18 de setembro de 2017, https://www.thenation.com/article/archive/the-children-of-the-arab-spring-are-being-jailed-and-tortured

229 Human Rights Watch, *Bahrain: Police Beat, Threaten Children*, 10 de março de 2021, https://www.hrw.org/news/2021/03/10/bahrain-police-beat-threaten-children

230 UNICEF, *UNICEF calls for the protection of children involved in Indonesia's protests*, 1 Outubro de 2019, https://www.unicef.org/press-releases/unicef-calls-protection-children-involved-indonesias-protests

231 Amnesty International, *Thailand: Urgent investigation needed after live rounds fired at child protesters*, 18 de Agosto de 2021, https://www.amnesty.org/en/latest/news/2021/08/thailand-urgent-investigation-needed-after-live-rounds-fired-at-child-protesters/

232 The Guardian, *Fear turns to fury in Myanmar as children shot by military*, 28 de Março de 2021, https://www.theguardian.com/global-development/2021/mar/28/fear-turns-to-fury-in-myanmar-as-children-shot-by-military

233 Veja, por exemplo: Freedom House, *Freedom in the World 2022*: United Kingdom, https://freedomhouse.org/country/united-kingdom/freedom-world/2022

234 Manchester Evening News, *Greater Manchester Police are collecting evidence against children protesting about climate change and threatening them with arrest*, 28 de Junho de 2019, https://www.manchestereveningnews.co.uk/news/greater-manchester-news/greater-manchester-police-collecting-evidence-16481957



**Cenário 2**

Xiu tem 15 anos e vive sob um regime no qual a censura na Internet é amplamente praticada. Para contornar a censura, críticos do regime têm usado o nome e a imagem de um personagem de desenho animado para fazer referência à liderança do país.[235] Xiu tenta usar essas referências para ler os textos de ativistas e se comunicar com outras pessoas com ideias semelhantes. Suas buscas e mensagens são escaneadas e bloqueadas.[236]

Este cenário mostra como a falta de criptografia pode colocar em risco o direito das crianças de buscar, receber e compartilhar informações, bem como se expressar sobre uma variedade de tópicos de interesse para elas. Alguns Estados, como a China, por meio de sua "*Grande Firewall*",[237]criaram sistemas complexos de censura *online*, que ameaçam diretamente os direitos das crianças. Um experimento de campo com estudantes universitários chineses sobre os efeitos de se ter acesso a uma Internet sem censura descobriu que "incentivos modestos e temporários para visitar portais de notícias ocidentais levaram a um aumento persistente na aquisição de informações politicamente sensíveis pelos estudantes" e que a "aquisição de informações politicamente sensíveis traz mudanças amplas, substanciais e persistentes no conhecimento, crenças, atitudes e comportamentos pretendidos dos estudantes", como discutir tópicos políticos com outras pessoas.[238]

A liberdade de expressão e informação é particularmente importante no contexto político atual, no qual o autoritarismo está em ascensão. Alguns especialistas temem que "a ordem global esteja chegando a um ponto de virada" e que, se a liberdade não for garantida, "o modelo autoritário prevalecerá".[239]E "a liberdade de expressão é o primeiro direito que líderes autoritários atacam ao minar a democracia", porque "a batalha definidora pelo poder é uma batalha para controlar a narrativa".[240] A importância da criptografia fica evidente em um mundo onde mais de um terço da população vive em países que "não são livres"[241] ou onde a liberdade de expressão está "em crise".[242]

235 This scenario was partly inspired by: BBC, *Why China censors banned Winnie the Pooh*, 17 July 2017, https://www.bbc.co.uk/news/blogs-china-blog-40627855

236 See, for example: The New York Times, *Apple's Compromises in China: 5 Takeaways*, 17 May 2021, https://www.nytimes.com/2021/05/17/technology/apple-china-privacy-censorship.html

237 See, for example: TechTarget, *Great Firewall of China*, https://www.techtarget.com/whatis/definition/Great-Firewall-of-China

238 Chen and Yang, *The Impact of Media Censorship: 1984 or Brave New World?*, American Economic Review 2019, 109(6): 2294–2332, pp. 2995-2996, https://www.gwern.net/docs/sociology/2019-chen.pdf

239 Freedom House, *Freedom in the World 2022: The Global Expansion of Authoritarian Rule*, https://freedomhouse.org/report/freedom-world/2022/global-expansion-authoritarian-rule

240 ARTICLE 19, *The Global Expression Report 2022: The intensifying battle for narrative control*, June 2022, p. 6, https://www.article19.org/wp-content/uploads/2022/06/A19-GxR-Report-22.pdf

241 Freedom House, *Freedom in the World 2022: The Global Expansion of Authoritarian Rule*.

242 ARTICLE 19, *The Global Expression Report 2022: The intensifying battle for narrative control*, June 2022, p. 5.

Quanto às crianças que fazem parte de grupos específicos, a criptografia é importante para proteger sua segurança uma vez que pertencer a comunidades desfavorecidas ou marginalizadas as expõe à violência estatal, como mostra o cenário a seguir.

**Cenário 3**
Amadou é um jovem gay de 17 anos. Em seu país, a homossexualidade é ilegal e estigmatizada, e membros da comunidade LGBT+ regularmente enfrentam violência do Estado e do público. Amadou usa serviços de mensagens não criptografadas para se encontrar com outros jovens LGBT+ e compartilhar informações sobre educação sexual. A polícia intercepta essas comunicações e Amadou é preso sob acusações de homossexualidade. A polícia então usa os contatos de Amadou para identificar e perseguir outros jovens LGBT+.[243]

A criptografia oferece benefícios específicos para jovens LGBT+ de países (por exemplo, os Emirados Árabes Unidos) que criminalizam a homossexualidade, bloqueiam conteúdo LGBT+ e monitoram salas de bate papo, mensagens instantâneas e blogs.[244] Ao mesmo tempo, defensores da proteção infantil enfatizaram que evidências sugerem que crianças que se identificam como LGBT+ e/ou com deficiência têm mais probabilidade de sofrer danos sexuais *online* durante a infância,[245] com jovens LGBT+ sendo pressionados a compartilhar imagens sexuais mais do que seus colegas heterossexuais.[246]

Quando crianças de grupos desfavorecidos ou marginalizados desejam denunciar os abusos sistêmicos a que são submetidas, a criptografia pode desempenhar um papel relevante, como mostra o próximo cenário.

**Cenário 4**
Ishaan, um jovem de 15 anos com deficiência, frequenta uma "escola especial" onde é constantemente intimidado, inclusive por funcionários da escola.[247] Ele escreve um artigo contundente que revela os abusos sofridos por ele e por outras crianças em sua escola, e critica o governo por suas políticas. Ele envia o artigo para várias pessoas, incluindo um jornalista, por mensagem direta. Todos eles o encaminham para diferentes plataformas. A história se torna viral, mas o jornalista se recusa a revelar sua fonte. No entanto, o governo tem uma lei de "rastreabilidade" que exige que os provedores de serviços eletrônicos sejam capazes de identificar o remetente de uma determinada mensagem.

243 Este cenário foi parcialmente inspirado por: Human Rights Watch, Cameroon: Wave of Arrests, Abuse Against LGBT People, 14 de abril 2021, https://www.hrw.org/news/2021/04/14/cameroon-wave-arrests-abuse-against-lgbt-people

244 VPN Overview, Censorship in the UAE: How to Get Around it, atualizado em 16 de novembro de 2022, https://vpnoverview.com/unblocking/censorship/internet-censorship-uae/

245 WeProtect Global Alliance, *Global Threat Assessment 2021*, p. 18.

246 Idem., p. 56.

247 Este cenário foi parcialmente inspirado por: The Guardian, Children with disabilities suffer 'severe neglect and abuse' in Australian schools, 27 de outubro de 2019, https://www.theguardian.com/society/2019/oct/28/children-with-disabilities-suffer-severe-neglect-and-abuse-in-australian-schools



Defensores da privacidade digital[248] e provedores de serviços de criptografia de ponta a ponta[249] alertaram que as disposições de rastreabilidade minam as garantias de privacidade e segurança da criptografia de ponta a ponta. Eles argumentam que, como não é possível saber antecipadamente quais mensagens os governos desejariam rastrear, as disposições de rastreabilidade efetivamente determinam que os serviços de mensagens, por meio de registros de metadados, mantenham o controle sobre quem enviou algo para quem e quando, para cada mensagem. Eles também alertam que essas disposições não são eficazes, uma vez que o remetente e o criador do conteúdo podem não ser a mesma pessoa - por exemplo, se uma pessoa simplesmente baixa uma imagem e a compartilha, ela seria considerada o remetente dessa imagem.[250]

Mas a criptografia de ponta a ponta ainda é fundamental para crianças que desejam expor injustiças. Como Edward Snowden colocou de forma simples, "teria sido impossível para mim fazer uma denúncia sem criptografia".[251]

### *Crianças que tomam decisões sobre seus próprios corpos*

Mesmo quando uma criança não é ativista e simplesmente quer fazer escolhas em relação ao seu próprio corpo, por exemplo, o Estado pode interferir em maneiras que podem colocar seus direitos em risco. Dessa forma, a criptografia é relevante para proteger esses direitos, como mostra o exemplo a seguir:

**Cenário 5**
Elena tem 12 anos e fica grávida após ser estuprada. Seu país criminaliza o aborto e não faz exceções para estupro ou incesto. Ela usa aplicativos de mensagens não criptografadas para encontrar um médico que realize um aborto em seu país e também busca *online* por clínicas de aborto em países vizinhos. Para coletar evidências criminais, o governo solicita às plataformas que verifiquem o conteúdo em busca de linguagem relacionada ao aborto. Também monitora buscas na *web* e identifica usuários que acessam material relacionado ao aborto.

248 Veja, por exemplo: EFF, *Why Indian Courts Should Reject Traceability Obligations*, 2 June 2021, https://www.eff.org/deeplinks/2021/06/why-indian-courts-should-reject-traceability-obligations; Access Now, *10 facts to counter encryption myths*, Agosto de 2021, https://www.accessnow.org/cms/assets/uploads/2021/08/Encryption-Myths-Facts-Report.pdf

249 WhatsApp, *What is traceability and why does WhatsApp oppose it?*, https://faq.whatsapp.com/2566310993676701/?locale=en_US

250 Ibidem.

251 Coalizão Global pela Criptografia, Edward Snowden and the Global Encryption Coalition say "Meddling with strong encryption puts public and economy at risk", 21 de outubro de 2021, https://www.globalencryption.org/2021/10/edward-snowden-and-the-global-encryption-coalition-say-meddling-with-strong-encryption-puts-public-and-economy-at-risk-press-release/

O debate sobre os direitos ao aborto tem como princípio central a integridade do corpo. É a ideia de que todos, incluindo crianças, têm o direito à autonomia e autodeterminação sobre o próprio corpo.[252] Essa é uma questão que é desproporcionalmente infringida no caso de crianças, que com mais frequência do que os adultos são submetidas a práticas em relação ao seu corpo em relação às quais não consentem.[253] Restrições não razoáveis ao aborto violam a integridade do corpo e também colocam em risco os princípios gerais que fundamentam a CDC, desde a não discriminação e o melhor interesse das crianças grávidas até o direito à vida e o direito de ser ouvido em assuntos que as afetam. Essas restrições também ameaçam uma série de outros direitos das crianças, como o direito à saúde, liberdade de informação, privacidade, liberdade de pensamento e o direito de estar livre de violência mental.[254]

Embora o Comitê tenha instado os Estados a descriminalizar o aborto para garantir que as meninas tenham acesso a abortos seguros e a serviços pós-aborto,[255] o aborto ainda é ilegal ou restrito em muitos países ao redor do mundo.[256] A criptografia, portanto, é particularmente importante para meninas grávidas com menos de 18 anos que desejam entender quais opções estão disponíveis para elas a fim de exercer seu direito de tomar decisões sobre seu próprio corpo, sem temer represálias.

O fato de que a criptografia tem implicações muito práticas para crianças grávidas é comprovado por um caso dos EUA, no qual foi relatado que o Facebook contribuiu com provas em um processo de aborto, entregando à polícia mensagens não criptografadas entre uma jovem grávida de 17 anos de Nebraska e sua mãe nas quais discutiam pílulas de aborto.[257] Especialmente diante da decisão da Suprema Corte dos EUA de revogar após quase 50 anos a proteção constitucional ao aborto de Roe versus Wade,[258] muitos especialistas em tecnologia nos EUA e em outros lugares pediram às empresas que limitem a extensão dos dados que coletam e retêm, que possam ser usados para obter informações sobre a saúde reprodutiva dos usuários[259] Uma das maneiras pelas quais as plataformas podem minimizar a quantidade de dados que coletam é expandindo a criptografia de ponta a ponta.

252 CRIN, *Bodily integrity*, https://home.crin.org/issues/bodily-integrity

253 Ibidem.

254 Para uma discussão sobre outros direitos envolvidos, veja: Human Rights Watch, Q&A: Access to Abortion is a Human Right, 24 de junho de 2022, https://www.hrw.org/news/2022/06/24/qa-access-abortion-human-right

255 Comitê dos Direitos da Criança da ONU, Comentário Geral No. 20 (2016) sobre a implementação de direitos da criança durante adolescência, CRC/C/GC/20, 6 de dezembro de 2016, § 60, https://www.refworld.org/docid/589dad3d4.html

256 Center for Reproductive Rights, *The World's Abortion Laws*, https://reproductiverights.org/maps/worlds-abortion-laws/

257 The Guardian, *Facebook gave police their private data. Now, this duo face abortion charges*, 10 de Agosto de 2022, https://www.theguardian.com/us-news/2022/aug/10/facebook-user-data-abortion-nebraska-police

258 *Dobbs v. Jackson Women's Health Organisation [Suprema Corte dos Estados Unidos], No. 19–1392, decidido em 24 de junho de 2022.*

259 The Guardian, Facebook gave police their private data. Now, this duo face abortion charges, 10 de Agosto de 2022.



### *Crianças desproporcionalmente afetadas por limitações gerais de direitos sob a lei*

De maneira mais geral, o debate sobre criptografia, crianças e o Estado também deve incluir uma discussão sobre as restrições aos direitos humanos que os governos podem impor sob o direito internacional e como os contornos dessas limitações podem afetar desproporcionalmente crianças de comunidades específicas, inclusive em países que não necessariamente têm características de autoritarismo.

Os direitos das crianças podem ser restringidos em estados de emergência. Por exemplo, o Pacto Internacional de Direitos Civis e Políticos estabelece que os Estados podem se afastar de suas obrigações de direitos humanos se isso for "estritamente necessário" durante um "estado de emergência pública que ameace a vida da nação" oficialmente proclamado.[260] A crise da COVID-19 já mostrou os perigos de os Estados utilizarem indevidamente decretos de emergência para irem além do que é necessário para conter a propagação da pandemia e, portanto, do que é permitido por lei.[261]

Fundamentalmente, as derrogações não devem "envolver discriminação apenas com base na raça, cor, sexo, língua, religião ou origem social".[262] Isso significa que, quando os governos limitam o uso da criptografia no contexto de um estado de emergência, a questão de saber se isso discrimina crianças de minorias étnicas e linguísticas, por exemplo, deve ser examinada cuidadosamente, como mostra o próximo cenário.

**Cenário 6**

Nina tem 16 anos e mora no País Urania, que faz fronteira com o País Ruritania. Nina pertence à minoria étnica Ruritana. Ela é bilíngue nas línguas Uraniana e Ruritania, como a grande maioria dos cidadãos de Urania, mas prefere falar Ruritania com sua família. Ruritania invade Urania, causando choque e condenação internacional. A letra A se torna um símbolo das forças pró-Ruritanas. O governo Uraniano declarou estado de emergência, proibiu a criptografia de ponta a ponta e exigiu que as plataformas identifiquem todos os usuários da língua Ruritana que compartilharam imagens da letra A. Nina compartilha em um grupo de bate-papo de sua família uma imagem da letra A grafitada em um prédio, denunciando aqueles que a desenharam. A conta de Nina é bloqueada e ela é denunciada às autoridades.

260 Art. 4, Pacto Internacional de Direitos Civis e Políticos.

261 Veja, por exemplo:: Special Rapporteurs and Independent Experts of the UN Human Rights Council, *COVID-19: States should not abuse emergency measures to suppress human rights – UN experts*, 16 de Março de 2020, https://www.ohchr.org/en/press-releases/2020/03/covid-19-states-should-not-abuse-emergency-measures-suppress-human-rights-un; Kriszta Kovács, *Hungary's Orbánistan: A Complete Arsenal of Emergency Powers*, 6 de Abril de 2020, https://verfassungsblog.de/hungarys-orbanistan-a-complete-arsenal-of-emergency-powers/; Radosveta Vassileva, *Bulgaria: COVID-19 as an Excuse to Solidify Autocracy?*, 10 de Abril de 2020, https://verfassungsblog.de/bulgaria-covid-19-as-an-excuse-to-solidify-autocracy/. Para uma discussão geral sobre COVID-19 e poderes de emergência, ver:Cassandra Emmons, *International Human Rights Law and COVID-19 States of Emergency*, 25 de Abril de 2020, https://verfassungsblog.de/international-human-rights-law-and-covid-19-states-of-emergency/

262 Pacto Internacional de Direitos Civis e Políticos

Mesmo quando a situação não atinge o nível de estado de emergência, o papel da criptografia deve ser discutido no contexto mais amplo de outras medidas estatais que limitam as liberdades fundamentais. Essas restrições ainda podem ameaçar os direitos das crianças, como a liberdade de informação, e afetar desproporcionalmente aqueles de comunidades específicas, como minorias religiosas, como o próximo cenário mostra.

**Cenário 7**

Leila tem 10 anos e é muçulmana. Ela fala abertamente sobre sua religião na escola. Quando um de seus colegas de escola a provoca e a chama de "noiva jihadista", ela quer entender mais sobre o que isso significa e usa um dos computadores da escola para procurar o termo. Em seu país, orientações do Departamento de Educação exigem que as escolas tenham filtros e sistemas de monitoramento para detectar sinais putativos de "radicalização". Suas buscas não criptografadas são sinalizadas[263] e ela é encaminhada para o programa do país projetado para evitar que as pessoas se tornem terroristas ou apoiem o terrorismo.

Um dos objetivos legítimos pelos quais os Estados podem restringir alguns direitos das crianças é a "proteção da segurança nacional",[264] mas essa disposição é suscetível a abusos pelos governos. No Reino Unido, por exemplo, no que diz respeito à prevenção do terrorismo, as orientações preveem o monitoramento das buscas *online* de crianças, mas falam pouco sobre a proteção de sua privacidade. Se forem identificadas erroneamente como "em risco de radicalização", as crianças são encaminhadas para o Prevent, um programa de combate ao terrorismo que tem como alvo desproporcional as crianças muçulmanas e representa sérios riscos para as liberdades fundamentais das crianças, algumas de suas práticas tendo sido consideradas violadoras de sua privacidade e seus direitos de dados.[265] Pesquisas criptografadas podem, portanto, ser uma maneira de proteger os direitos das crianças de minorias religiosas. Ao mesmo tempo, indivíduos e grupos que tentam manipular crianças e organizar violência política usam canais criptografados para fazê-lo. As discussões de políticas sobre os benefícios e riscos da criptografia para os direitos das crianças precisam levar em conta essas especificidades.

## Criptografia, crianças e suas famílias

No caso de crianças e suas famílias, o debate sobre o papel da criptografia deve levar em consideração pelo menos dois contextos que até agora receberam pouca atenção:

263 O termo "noiva de jihad" aparece numa lista de palavras-chave que o software pode sinalizar: The Guardian, Schools monitoring pupils' web use with 'anti-radicalisation software', 10 de Junho de 2015, https://www.theguardian.com/uk-news/2015/jun/10/schools-trial-anti-radicalisation-software-pupils-internet

264 Veja, por exemplo, o Art. 13 da Convenção sobre os Direitos da Criança.

265 Para a discussão sobre Prevent e direitos da criança, incluindo um foco particular nos dados da criança, veja CRIN, Preventing Safeguarding: The Prevent strategy and children's rights, março de 2022, https://static1.squarespace.com/static/5afadb22e17ba3eddf90c02f/t/62385835c6d6f61c4977be26/1647859768092/Preventing+Safeguarding+March+2022+CRIN.pdf



o caso de crianças cujos interesses ou opiniões diferem dos de seus pais e o caso de crianças que podem estar em desvantagem devido ao status de seus pais.
O Comitê reconheceu que "[o] ambiente digital apresenta problemas particulares para os pais e cuidadores no que concerne ao respeito pelos direitos das crianças à privacidade" e mencionou especificamente os riscos apresentados pelas "[t]ecnologias que monitoram as atividades online por motivos de segurança".[266]

Ele também reconheceu que "[a] proteção da privacidade de uma criança no ambiente digital pode ser vital em circunstâncias em que os pais ou cuidadores representem uma ameaça à segurança da criança".[267] O debate sobre criptografia deve levar isso em consideração. Como o próximo cenário mostra, por exemplo, em casos de violência doméstica, tecnologias de monitoramento podem colocar crianças em risco.

**Cenário 8**

Cora, uma criança de 9 anos, tem uma mãe abusiva. Ela não conta isso a nenhum parente, temendo que ninguém acredite nela e que alertem sua mãe. No entanto, ela tira fotos das contusões em seu corpo nu para ajudar a evidenciar o abuso e tenta enviá-las a um amigo cuja família trabalha na polícia.
O telefone sinaliza as fotos e notifica sua mãe.

Este exemplo destaca como crianças vítimas de violência doméstica podem ser colocadas em risco por iniciativas de escanear o conteúdo de seus telefones em busca de abuso sexual ou sinais de aliciamento e, em seguida, notificar os pais. O processo de detecção automática pode ser excessivamente abrangente, porque a contextualização necessária, que seria mais evidente para um revisor humano, está ausente. Imagens podem ser sinalizadas como evidência de violência, mas na verdade não indicarem abuso sexual ou aliciamento. Portanto, os pais abusivos podem ser alertados quando as crianças tentam buscar ajuda e enviar evidências. Isso colocaria as crianças em maior risco de violência devido ao potencial de retaliação.

A comunicação segura é especialmente importante para crianças que são vítimas de violência doméstica, pois permite que elas se comuniquem de forma segura com pessoas de fora de suas casas em quem confiam, por exemplo, para buscar ajuda. Se as crianças armazenarem e enviarem evidências de abuso usando criptografia, os agressores não podem interceptá-las, nem adulterá-las. Isso preserva a privacidade das crianças e as protege da violência física e mental perpetrada pelos agressores.[268]

266 Comitê dos Direitos da Criança da ONU, Comentário Geral No. 25 (2021) sobre os direitos da criança em relação ao ambiente digital, CRC/C/GC/25, 2 de março de 2021, § 76.

267 Idem., para. 77.

268 A importância da criptografia para vítimas e sobreviventes de violência doméstica, violência sexual, *stalking* e tráfico é discutida em mais detalhes aqui: ISOC, Fact Sheet: Understanding Encryption: The Connections to Survivor Safety, 18 de dezembro de 2020, https://www.internetsociety.org/resources/doc/2020/understanding-encryption-the-connections-to-survivor-safety/

Mesmo que os pais não representem necessariamente uma ameaça às crianças, as tecnologias de monitoramento podem criar dificuldades para elas, especialmente se começarem a desenvolver opiniões diferentes das de seus pais, como exemplificado no seguinte cenário.

**Cenário 9**

Alex tem 12 anos e vem de uma família muito conservadora. Alex foi designado como do sexo feminino ao nascer. No entanto, elu vem questionando sua identidade de gênero há algum tempo. Preocupado com as mudanças pelas quais seu corpo está passando, elu começou a ler sobre maneiras de fazer com que pareça menos feminino. Um dia, quando seus pais não estão em casa, Alex aperta o peito e envia uma foto a um amigo em quem confia. Seu telefone sinaliza o conteúdo como sexualmente explícito, e seus pais são notificados e recebem uma cópia da foto.[269]

A CDC afirma que os pais têm responsabilidades, direitos e deveres de orientar seus filhos "de maneira consistente com as capacidades em desenvolvimento da criança" (Art. 5º). Na medida em que as crianças têm a capacidade de tomar decisões por si mesmas, essas decisões devem ser respeitadas. O Comitê reconheceu especificamente que "[o] monitoramento da atividade digital de pais e cuidadores de crianças deve ser [...] de acordo com as capacidades em desenvolvimento da criança".[270]

Tecnologias que monitoram as comunicações de crianças colocam algumas delas, por exemplo, aquelas que pertencem à comunidade LGBT+, em uma posição difícil. Essas tecnologias correm o risco de violar a privacidade das crianças ao revelar sua orientação sexual ou identidade de gênero aos pais quando elas não estão prontas ou dispostas a discutir sua identidade sexual. Essas crianças também correm risco elevado de violência e abuso, como serem expulsas de casa, se seus pais não aceitarem sua identidade.[271] Como vítimas de violência doméstica, a comunicação criptografada de ponta a ponta é, portanto, especialmente importante para crianças LGBT+.

O debate sobre criptografia e direitos das crianças também deve destacar um grupo de crianças que até agora recebeu pouca atenção: aquelas que podem sofrer discriminação com base em quem são seus pais, como o próximo cenário explora.

269 Este cenário foi adaptado de um exemplo hipotético dado por Jillian York da EFF. Ver The Center for Public Integrity, Proposed iPhone protections could put LGBTQ youth at risk, 24 de setembro de 2021, , https://publicintegrity.org/inside-publici/newsletters/watchdog-newsletter/iphone-protections-lgbtq-youth/

270 Comitê dos Direitos da Criança da ONU, Comentário Geral No. 25 (2021) sobre os direitos da criança em relação ao ambiente digital, CRC/C/GC/25, 2 de março de 2021, § 76.

271 Este ponto foi feito em: The Center for Public Integrity, Proposed iPhone protections could put LGBTQ youth at risk, 24 de setembro de 2021.



**Cenário 10**

Dev tem 8 anos e é filho de uma mãe solteira que é portadora de HIV.[272] Sua mãe usa plataformas não criptografadas para se conectar com outras pessoas e compartilhar informações sobre prevenção e tratamento de HIV. Ela não divulga sua condição com medo de que possa perder a guarda de seu filho. O Estado faz esforços para rastrear todas as pessoas com HIV, incluindo monitorar as comunicações em plataformas *online*, e identifica a mãe de Dev. Toda a escola fica sabendo. Sua professora o faz sentar separadamente de seus colegas e vários de seus colegas começam a abusar verbalmente dele.

A CDC reconhece que as crianças estão em uma posição particular porque seu status muitas vezes está associado ao de seus pais. O Art 2º da CDC proíbe a discriminação com base em "raça, cor, sexo, língua, religião, opinião política ou de outra natureza, origem nacional, étnica ou social, propriedade, deficiência, nascimento ou outro status da criança *ou de seus pais ou responsáveis legais* [ênfase adicionada]". Também exige que a criança seja protegida contra "discriminação ou punição com base no status [ênfase adicionada], atividades, opiniões expressas ou crenças dos pais, responsáveis legais ou membros da família".

As crianças de pais portadores de HIV frequentemente enfrentam estigmatização, discriminação e "são negadas o acesso a informações, educação, saúde ou serviços de assistência social ou vida comunitária".[273] Portanto, elas correm risco particular se o Estado revelar o status de HIV dos pais quando eles não podem usar a criptografia para se comunicar de forma segura.

## Criptografia, crianças e empresas

O debate sobre criptografia e direitos das crianças destaca a importância de empresas como plataformas de redes  sociais e deve levar em conta os contextos nos quais elas desempenham um papel desproporcional. Como o cenário a seguir mostra, por exemplo, a criptografia de ponta a ponta pode representar sérios riscos ao direito das crianças de serem protegidas da violência quando plataformas criptografadas de rede social são usadas para incitar violência *offline.*

272 Este cenário foi parcialmente inspirado por: RAND Corporation, How Parental HIV Affects Children, 2009https://www.rand.org/pubs/research_briefs/RB9372.html

273 Comitê dos Direitos da Criança da ONU, Comentário Geral No. 3 (2003): HIV/AIDS e os direitos da criança, CRC/GC/2003/3, 17 de março de 2003, § 7, https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsiQql8gX5Zxh0cQqSRzx6ZeEf9bA8YygWAWhjeBgKhcc0njrT-tlx20RETRkrClf0qEtVlKxay%2FFwzytKp1XPhB%2F6joKO6UVePMIHldiwQtwk

**Cenário 11**

Sophia tem 13 anos e pertence a um grupo étnico minoritário que está constantemente sendo alvo de discursos de ódio em plataformas de rede social criptografadas de ponta a ponta. Como resultado, houve um aumento substancial no número de ataques violentos contra membros do grupo étnico de Sophia, e ela fica relutante em expressar sua própria identidade e opiniões com medo de ser sujeita a abusos.

As empresas desempenham um papel crucial no ambiente digital, mas existem alguns contextos políticos, sociais e econômicos nos quais sua influência é tão significativa que, estejam elas criptografadas ou não, desproporcionalmente envolvem os direitos das crianças. Um dos exemplos mais conhecidos é o papel do *Facebook* em Mianmar. Muitos viam o *Facebook* como "a internet em Mianmar"[274] porque era a principal fonte de informação e um meio para as autoridades se comunicarem com o público. No entanto, diante da violência que eclodiu contra a minoria muçulmana Rohingya, um relatório da missão independente internacional de investigação sobre Mianmar, estabelecida pelo Conselho de Direitos Humanos da ONU, descobriu que o *Facebook* foi "um instrumento útil para aqueles que buscam disseminar o ódio" e que a resposta da empresafoi "lenta e ineficaz".[275] Uma ação coletiva de 150 bilhões de libras esterlinas movida pelos Rohingya contra a empresa alega que seus algoritmos amplificaram discursos de ódio contra o grupo minoritário e que houve falta de investimento em moderadores locais de conteúdo que entenderiam o idioma e o contexto cultural. Ela também acusa o *Facebook* de não remover postagens específicas incitando a violência e de não desativar contas, grupos e páginas que estavam fomentando tensões.[276]

Vale ressaltar que todos esses problemas estavam presentes em um ambiente que não era criptografado de ponta a ponta. A criptografia de ponta a ponta tornaria esses problemas ainda mais difíceis de serem abordados, pois remove a capacidade das plataformas de detectar conteúdo problemático. Isso mostra o impacto desproporcional que a criptografia de plataformas influentes tem nos direitos das crianças, especialmente quando pertencem a grupos minoritários.

Até agora, o foco principal no debate sobre criptografia e direitos das crianças tem sido sobre o conteúdo das comunicações, e não sobre outros dados, como a localização atual das crianças, endereço, registros de chamadas e mensagens etc.[277]

274 BBC, *Myanmar coup: How Facebook became the 'digital tea shop'*, 4 de Fevereiro de 2021, https://www.bbc.co.uk/news/world-asia-55929654

275 Relatório da missão internacional independente de investigação sobre Mianmar, A/HRC/39/64, 12 de setembro de 2018, p. 14, https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/FFM-Myanmar/A_HRC_39_64.pdf

276 The Guardian, Rohingya sue Facebook for £150bn over Myanmar genocide, 6 de dezembro de 2021, https://www.theguardian.com/technology/2021/dec/06/rohingya-sue-facebook-myanmar-genocide-us-uk-legal-action-social-media-violence

277 Kardefelt-Winther, D. et al., Encryption, Privacy and Children's Right to Protection from Harm, 2020, UNICEF Office of Research – Innocenti Working Paper 2020-14, p. 7.



No entanto, o acesso a metadados também requer atenção, especialmente no contexto das atividades empresariais e dos direitos das crianças. Isso ocorre porque, mesmo que o conteúdo das comunicações da criança seja criptografado de ponta a ponta, as empresas podem coletar esses dados sobre as crianças, usá-los e compartilhá-los para obter lucro.[278]

Além do contexto empresarial, em qualquer caso, os metadados também podem ser reveladores, como foi argumentado na discussão sobre disposições de rastreabilidade. Como o cenário a seguir mostra, por exemplo, ele também pode ser usado por agressores de uma maneira que coloca as crianças em risco de violência.

**Cenário 12**

Juan tem 14 anos e é um ativista ambiental indígena. Ele faz parte de um grupo desarmado que patrulha terras indígenas para garantir que grupos armados não asinvadam e saqueiem.[279] Um membro de um grupo armado rouba o telefone de Juan e usa dados não criptografados sobre suas localizações anteriores para determinar qual rota a patrulha indígena pegará em seguida. A patrulha é então emboscada violentamente pelo grupo armado.

Os termos do debate sobre criptografia e direitos das crianças, portanto, devem ser ampliados para levar em consideração não apenas a criptografia do conteúdo, mas também a criptografia dos metadados, e considerar suas implicações em contextos diversos.

278 Ibidem.

279 Esta parte do cenário foi inspirada por um caso real: The Guardian, Shock in Colombia over murder of 14-year-old indigenous activist, 18 de janeiro de 2022, https://www.theguardian.com/global-development/2022/jan/18/colombia-indigenous-activist-murdered-14-breiner-david-cucuname

# Propostas legislativas

Nos últimos anos, tem havido um aumento no número de propostas legislativas e outras iniciativas em torno do ambiente digital que têm impacto na criptografia, muitas vezes com o objetivo de manter as pessoas seguras.[280]

O Relator Especial da ONU para a liberdade de expressão identificou em 2018 uma variedade de tendências nas restrições estatais à encriptação. [281]

- Alguns adotaram leis penais que proíbem a utilização de criptografia, como o Irã por meio da sua *Computer Crimes Act* [Lei de Crimes Informáticos].
- Alguns, como a Rússia, aprovaram leis que exigem o registro e a aprovação governamental de ferramentas de encriptação.
- Alguns países apresentaram *frameworks* para o fornecimento de acesso às comunicações às agências de aplicação da lei e de segurança. Por exemplo, a Lei de Cibersegurança da China exige que os operadores de rede prestem "apoio e assistência técnica" aos órgãos de segurança pública e nacional. *A Investigatory Powers Act* [Lei de Poderes de Investigação] do Reino Unido de 2016, complementada pelas regulações secundárias de 2018, permite que as autoridades emitam um "aviso de capacidade técnica" para serviços *online*, o que pode obrigá-los a criar *backdoors* e remover criptografia de ponta a ponta. Foi apelidada de "*the Snoopers' Charter*" [Carta dos Bisbilhoteiros] por defensores da privacidade e foi descrita como "o regime de vigilância mais intrusivo e menos responsável do Ocidente" por Edward Snowden em 2015. [282] A Austrália seguiu o exemplo, aprovando a "*Assistance and Access Act 2018*" [Lei de Assistência e Acesso de 2018], que exige que prestadores de serviços desenvolvam capacidade técnica para ajudar as agências de aplicação da lei e de inteligência. Uma proposta semelhante nos EUA, a *Encrypted Data Act* [Lei de Acesso Legal a Dados Criptografados], foi apresentada em 2020.
- Outros Estados utilizaram a criptografia como justificativa para instituir amplos regimes contra o *hacking*, ou exigiram que serviços *online* armazenassem localmente dados pessoais ou sensíveis, incluindo chaves de encriptação.
- Ainda outros, como a Índia e o Brasil, propuseram requisitos de rastreabilidade, solicitando aos prestadores de serviços que sejam capazes de identificar o remetente original de uma mensagem. [283]

---

280 Para uma visão geral das discussões regulatórias recentes, consulte Tech Against Terrorism, Terrorist Use of E2EE: State of Play, Misconceptions, and Mitigation Strategies, 2021; Para uma visão global do status legal da criptografia, consulte Global Partners Digital, , World map of encryption laws and policies, https://www.gp-digital.org/world-map-of-encryption/

281 Relatório do Relator Especial sobre a Promoção e Proteção do Direito à Liberdade de Opinião e Expressão como seguimento do relatório de 2015 sobre o uso de criptografia e anonimato para exercer os direitos à liberdade de opinião e expressão na era digital, A /HRC/38/35/Add.5, 13 de julho de 2018,https://digitallibrary.un.org/record/1638475?ln=en

282 Veja seus comentários no Twitter em: https://twitter.com/snowden/status/661950808381128704

283 Veja Tech Against Terrorism, Terrorist Use of E2EE: State of Play, Misconceptions, and Mitigation Strategies, 2021, pp. 33-34.

A primeira tentativa de legislação para segurança *online* veio da Austrália em 2015, com a sua *Enhancing Online Safety Act* [Lei de Melhoria da Segurança Online] . Ela foi atualizada em 2021 pela *Online Safety Act* [Lei de Segurança Online], que entrou em vigor em janeiro de 2022.[284] Essa fornece um conjunto de Expectativas Básicas de Segurança Online para serviços online que os responsabilizam pela segurança dos usuários. Exige também que a indústria desenvolva códigos obrigatórios para conteúdos ilegais e restritos, o que pode exigir que as plataformas removam material de abuso sexual infantil e coloca maior pressão sobre os serviços *online* para proteger as crianças de conteúdos que não sejam apropriados para a idade. A Lei confere poderes consideráveis ao *eSafety Commissioner* [Comissário de Segurança Eletrônica], que pode impor normas para a indústria se não for alcançado acordo sobre os códigos ou se as normas desenvolvidas não forem adequadas.

Indiscutivelmente, 2022 foi o ano mais importante até agora para discussões regulatórias sobre a proteção das crianças *online*, especialmente contra o abuso e a exploração sexual. Três propostas foram apresentadas e estão atualmente em discussão nos EUA, no Reino Unido e na UE. Os seus objetivos são incontroversos, mas as sugestões para manter as crianças seguras e o impacto que estas sugestões têm na criptografia (de ponta a ponta) estão dando origem a divergências.

**Lei dos EUA para eliminação da negligência abusiva e desenfreada de tecnologias interativas de 2022 (EARN IT Act de 2022)**[285]

| Mudanças previstas na proposta | Áreas de desacordo em relação à criptografia e aos direitos das crianças |
|---|---|
| A Lei EARN IT de 2022 foi apresentada em janeiro. A versão original do projeto de lei havia sido elaborada em 2020.<br><br>A lei cria a Comissão Nacional de Prevenção da Exploração Sexual Infantil Online, cujo objetivo é "desenvolver recomendações de melhores práticas" que as plataformas podem optar por implementar para "prevenir, reduzir e responder à exploração sexual online de crianças".[286] | O objetivo da Lei EARN IT de 2022 é lutar contra a exploração sexual online de crianças.<br><br>No entanto, tem havido avisos de que a lei ameaça a privacidade de todos os usuários, que poderia levar à remoção excessiva de conteúdos e que poderia tornar mais difícil processar aqueles que exploram crianças *online*.[287]<br><br>Há preocupações de que a lei possa impor, com efeito, uma obrigação de monitoramento às plataformas. |

284 Australian eSafety Commissioner, *Online Safety Act 2021 - Fact sheet*, Julho de 2021, https://www.esafety.gov.au/sites/default/files/2021-07/Online%20Safety%20Act%20-%20Fact%20sheet.pdf

285 Disponível em: https://www.congress.gov/bill/117th-congress/senate-bill/3538/text

286 Seção 3 do EARN IT Act de 2022.

287 Veja, por exemplo: Riana Pfefferkorn, The EARN IT Act Is Back, and It's More Dangerous Than Ever, 4 de Fevereiro de 2022, https://cyberlaw.stanford.edu/blog/2022/02/earn-it-act-back-and-it%E2%80%99s-more-dangerous-ever; Jeffrey Westling, *Unintended Consequences of the EARN IT Act*, 23 de Fevereiro de 2022, https://www.americanactionforum.org/insight/unintended-consequences-of-the-earn-it-act/



| | |
|---|---|
| A Lei também altera a Seção 230 da Lei das Comunicações de 1934, o atual regime de responsabilidade dos intermediários *online*.[288]<br><br>Atualmente, a Seção 230 impede que as plataformas sejam tratadas como editoras ou porta-vozes do que os usuários postam online. Nenhuma responsabilidade pode ser imposta em lei que seja inconsistente com esta seção. No entanto, ao abrigo da Seção 230, a imunidade das plataformas não se estende à legislação penal federal relativa à exploração sexual de crianças. Constitui crime federal que as plataformas possuam ou compartilhem conscientemente material de abuso sexual infantil.[289] As plataformas também são obrigadas a relatar esse tipo material em seus serviços de que tenham conhecimento.[290]<br><br>A Lei EARN IT remove a imunidade das plataformas em relação à "publicidade, promoção, apresentação, distribuição ou solicitação" de material de abuso sexual infantil em ações civis e criminais sob a lei estadual.[291] No entanto, nenhum dos três fatores seguintes - o fato de as plataformas utilizarem criptografia de ponta aponta ou de outra forma nos seus serviços, de não possuírem as informações necessárias para descriptografar uma comunicação ou de não tomarem medidas que prejudiquem a sua capacidade de oferecer criptografia de ponta a ponta ou outra criptografia - pode ser uma "base independente para responsabilidade". Os tribunais podem considerar provas relativas a esses três fatores se forem admissíveis de outra forma.[292] | Isto porque, embora ao abrigo da lei federal o padrão de responsabilidade seja o conhecimento real de material de abuso sexual infantil, as leis estaduais podem ter um padrão inferior, como imprudência ou negligência relativamente à sua existência. Assim, uma plataforma que não tem conhecimento da existência de material de abuso sexual infantil nos seus serviços pode ser responsabilizada sob a legislação estadual se ela devesse ter tido conhecimento ou fosse negligente em relação à existência desse material. A preocupação é que os requerentes ou os procuradores possam argumentar, por exemplo, que a oferta de serviços de encriptação não é uma base independente para a responsabilidade, mas é um dos fatores que contribuem para o comportamento imprudente da plataforma. Por conseguinte, a fim de evitar litígios dispendiosos e morosos, as plataformas poderão ser pressionadas a enfraquecer ou remover a encriptação dos seus serviços. Elas também podem ser incentivados a usar a varredura pelo lado do cliente para detectar material de abuso sexual infantil antes que a comunicação seja criptografada ou depois de descriptografada.<br><br>Os críticos também alertam que a lei delegaria às plataformas poderes de agentes do governo, tornando as provas obtidas por elas inadmissíveis em tribunal ao abrigo da Quarta Emenda à Constituição dos EUA, que proíbe as "buscas e apreensões injustificadas" de comunicações de indivíduos pelas autoridades policiais sem um mandado judicial.[293] |

288 Veja no Título 47 do US Code: 47 U.S.C. 230 (e), disponível em: https://www.law.cornell.edu/uscode/text/47/230

289 Seção 2252A, disponível em: https://www.law.cornell.edu/uscode/text/18/2252A

290 Seção 2258A, disponível em: https://www.law.cornell.edu/uscode/text/18/2258A

291 Seção 5 do EARN IT Act de 2022. Também autoriza ações civis federais por conduta que viole as Seções 2252 ou 2252A do Código dos EUA.

292 Seção 5 do EARN IT Act de 2022.

293 Disponível em: https://www.law.cornell.edu/constitution/fourth_amendment

| Lei de Segurança Online (Reino Unido)[294] | |
|---|---|
| **Mudanças previstas na proposta** | **Áreas de desacordo em relação à criptografia e aos direitos das crianças** |
| O Governo do Reino Unido apresentou a Lei de Segurança Online na Câmara dos Comuns em março de 2022. O projeto havia sido proposto em maio de 2021, como resposta à consulta pública sobre o relatório "Online Harms White Paper", de abril de 2019. Em 2022, o Governo do Reino Unido investiu 500 mil libras esterlinas[295] na campanha "*No Place to Hide*",[296] que pedia às empresas de redes sociais que se comprometessem a implementar criptografia de ponta-a ponta somente quando "tivessem a tecnologia para garantir que as crianças não corram riscos maiores como resultado".<br><br>A Lei de Segurança Online impõe deveres de cuidado aos provedores de serviços de usuário para usuário e de serviços de busca.[297] Todos esses provedores têm o dever de lidar com conteúdos ilegais, como a exploração e o abuso sexual infantil, conduzindo avaliações de risco e tomando medidas proporcionais para mitigar e gerir de forma eficaz o risco de danos aos indivíduos.[298] Por exemplo, os serviços de usuário para usuário têm o dever de impedir que os indivíduos se deparem com conteúdos de exploração e abuso sexual infantil, minimizar o tempo durante o qual esse conteúdo está em circulação e derrubá-lo rapidamente assim que tomarem conhecimento dele.[299] Todo conteúdo desse tipo que fordetectado deve ser denunciado à Agência Nacional do Crime.[300] | A Lei de Segurança Online pretende cumprir o compromisso de "tornar o Reino Unido o lugar mais seguro do mundo para se estar online", inclusive para crianças.[301]<br><br>As preocupações em torno da Lei de Segurança Online centram-se no fato de, na prática, parecer impor uma obrigação geral de monitoramento, mesmo para provedores de serviços que utilizam criptografia de ponta a ponta. A fim de cumprir os deveres de avaliação de risco e moderação de conteúdo, bem como quaisquer requisitos do Ofcom, os provedores de serviços precisariam verificar todo o conteúdo do usuário. A incapacidade de distinguir entre plataformas públicas e serviços de mensageria privada significa que a oferta de criptografia de ponta a ponta pode violar os deveres do projeto de lei.[302]As plataformas podem ter que utilizar a verificação pelo lado do cliente antes de a comunicação ser encriptada ou depois de ser desencriptada.<br><br>De forma mais ampla, os críticos alertaram que o projeto de lei se concentra demais na moderação de conteúdo em vez de abordar o modelo de negócios das plataformas (a monetização da atenção dos usuários), delega às plataformas a tomada de decisões sobre a ilegalidade do conteúdo, |

294 Disponível em: https://bills.parliament.uk/bills/3137. A análise baseia-se no texto do Projeto de Lei em 5 de dezembro de 2022.

295 Computer Weekly, *Government funds charity campaign to warn big tech over the risks of encryption to children*, 19 de Janeiro de 2022, https://www.computerweekly.com/news/252512196/Government-funds-charity-campaign-to-warn-big-tech-over-the-risks-of-encryption-to-children

296 Disponivel em: https://noplacetohide.org.uk/

297 Veja, por exemplo, as seções 2, 6, 7, 22, 23 do Online Safety Bill.

298 Veja, por exemplo, as seções 8, 9, 24, 25 do Online Safety Bill.

299 Seção 9 do Online Safety Bill.

300 Seção 60 do Online Safety Bill.

301 Governo do Reino Unido, Lei de Segurança Online: ficha informativa, última atualização em 19 de abril de 2022, https://www.gov.uk/government/publications/online-safety-bill-supporting-documents/online-safety-bill-factsheet

302 Veja, por exemplo: ARTIGO 19, UK: Online Safety Bill is a serious threat to human rights online, 25 de abril de 2022, https://www.article19.org/resources/uk-online-safety-bill-serious-threat-to-human-rights-online/



| | |
|---|---|
| Além disso, os serviços de usuário a usuário e os serviços de busca que possam ser acessados por crianças devem realizar uma avaliação de impacto às crianças e tomar medidas proporcionais para protegê-las de conteúdo que lhes é prejudicial.[303] Isto será definido pelo Secretário de Estado em regulação secundária.[304]<br><br>Ofcom, o regulador de comunicações do Reino Unido, pode impor um "requisito de tecnologia proativa" a um serviço com o objetivo de fazercumprir seus deveres em relação a conteúdo ilegal e à segurança *online* de crianças.[305] Além disso, o Ofcom pode demandar de um provedor de serviços que utilize "tecnologia credenciada" para identificar e eliminar rapidamente conteúdos de exploração e abuso sexual infantil, quer sejam comunicados publicamente ou no privado.[306] Ao decidir se é necessária e proporcional uma ordem dessa natureza, o Ofcom deve considerar uma série de fatores, incluindo o tipo de serviço, as suas funcionalidades, a sua base de usuários, a prevalência e disseminação do conteúdo, o risco e a gravidade dos danos, os sistemas e processos utilizados pelo serviço para identificar e remover o conteúdo e os riscos à liberdade de expressão e privacidade dos usuários.[307]<br><br>O Ofcom pode solicitar aos provedores de serviços quaisquer informações de que necessite para exercer ou decidir sobre o exercício de suas funções.[308] É crime fornecer ao Ofcom informações criptografadas, ininteligíveis, com a intenção de impedir o órgão de compreender essas informações.[309] | infringe a liberdade de expressão e privacidade dos usuários ao encobrir conteúdo "danoso" que não é ilegal e põe em perigo a independência do Ofcom ao dar demasiado poder ao Secretário de Estado sobre a implementação do projeto de lei.[310]<br><br>Do ponto de vista dos direitos das crianças, é preocupante que tanto poder esteja nas mãos do Ofcom, já que o órgão não tem conhecimentos específicos nessa área. |

303 Veja, por exemplo, as seções 10, 11, 26, 27 do Online Safety Bill.

304 Seção 54 do Online Safety Bill.

305 Seção 120 do Online Safety Bill.

306 Seção 106 do Online Safety Bill.

307 Seção 108 do Online Safety Bill.

308 Seção 87 do Online Safety Bill.

309 Seção 94 do Online Safety Bill

310 ARTIGO 19, UK: Online Safety Bill is a serious threat to human rights online, 25 de abril de 2022.

| Proposta da UE para um "Regulamento que estabelece regras para prevenir e combater o abuso sexual de crianças"[311] | |
|---|---|
| **Mudanças previstas na proposta** | **Áreas de desacordo em relação à criptografia e aos direitos das crianças** |
| A proposta da UE para um Regulamento sobre Abuso Sexual Infantil ("CSAR") foi apresentada em maio de 2022.<br><br>A proposta foi desenvolvida no contexto da estratégia da UE para uma luta mais eficaz contra o abuso sexual de crianças, que foi adotada em julho de 2020.[312]Fornece um quadro para o desenvolvimento de uma resposta abrangente ao abuso sexual de crianças online e offline. A estratégia estabelece várias iniciativas, incluindo a garantia da implementação completa da legislação atual, como a Diretiva contra Abuso Sexual de Crianças[313]; a identificação de lacunas e a proposta de nova legislação; o reforço de aplicação da lei e de ações preventivas; e a criação de um centro europeu para prevenir e combater o abuso sexual de crianças. Em novembro de 2020, o Conselho da UE emitiu uma resolução sobre "Segurança através da criptografia e segurança apesar da criptografia"[314] Em julho de 2021, a UE adotou uma derrogação temporária à Diretiva sobre Privacidade Eletrônica[315] , permitindo aos provedores de serviços tomar medidas voluntárias para deletar, denunciar e remover material de abuso sexual infantil. Em outubro de 2022, a UE adotou a Lei dos Serviços Digitais[316], que alterou uma diretiva de 20 anos atrás[317] que se aplicava aos serviços online. | Como pano de fundo, existe um cenário complexo no que diz respeito às abordagens das várias iniciativas e leis da UE para a criptografia de ponta a ponta. A estratégia da UE para uma luta mais eficaz contra o abuso sexual de crianças reconhece a utilização da criptografia para fins criminosos e apela a "possíveis soluções que possam permitir às empresas detectar e denunciar o abuso sexual de crianças em comunicações eletrônicas criptografadas de ponta aponta".[318] A Resolução do Conselho da UE sobre Criptografia refere-se a "soluções técnicas para obter acesso a dados criptografados", observando que elas devem respeitar os "princípios de legalidade, transparência, necessidade e proporcionalidade, incluindo a proteção de dados pessoais desde a concepção e por padrão".<br><br>Por outro lado, o texto da derrogação temporária da Diretiva sobre Privacidade Eletrônica afirma especificamente que nada nele deve ser interpretado para "proibir ou enfraquecer a criptografia de ponta a-ponta"[319]. A Lei dos Serviços Digitais mantém a proibição de monitoramento geral, o que significa que não pode ser solicitado dos provedores de serviços que monitorem as informações transmitidas ou armazenadas, ou procurem ativamente circunstâncias que indiquem ilegalidade. [320] |

311 Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN

312 Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:607:FIN

313 Diretiva 2011/93/EU, disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02011L0093-20111217

314 Disponível em: https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/en/pdf

315 Regulação(EU) 2021/1232, disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R1232

316 Regulação (EU) 2022/2065, disponível em: https://eur-lex.europa.eu/eli/reg/2022/2065/oj

317 Diretiva sobre comércio eletrônico ou E-Commerce Directive 2000/31/EC, disponível em: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031

318 Introdução à Estratégia.

319 Recital 25 da derrogação temporária.

320 Art. 8 do Digital Services Act.



| | |
|---|---|
| O CSAR da UE estabelece regras para abordar "a utilização indevida de serviços relevantes da sociedade da informação para o abuso sexual de crianças *online*".[321] Esses serviços são definidos como: serviços de hospedagem, serviços de comunicações interpessoais, lojas de aplicativos de *software* e serviços de acesso à Internet.[322]<br><br>O CSAR impõe obrigações de avaliação, mitigação e comunicação de riscos aos serviços de hospedagem e comunicação interpessoal relativamente ao abuso sexual infantil *online*. Isso abrange a "divulgação de material previamente detectado e confirmado como constituindo material de abuso sexual infantil (material 'conhecido'), além do material não detectado anteriormente que possa constituir material de abuso sexual infantil, mas que ainda não foi confirmado como tal ('novo' material), bem como atividades que constituem aliciamento de crianças ('*grooming*').[323]<br><br>Ao conduzir uma avaliação de risco relativa ao abuso sexual de crianças *online*, os serviços devem levar em conta, entre outros fatores, diversas funcionalidades para fazer face ao risco, tais como proibições e restrições estabelecidas em termos e condições e formas de as aplicar, mecanismos deverificação de idade e ferramentas de denúncia.[324] | O Parlamento da UE havia aprovado texto protetivo criptografia de ponta a ponta, mas ele não foi incluído na versão final da Lei dos Serviços Digitais.[325]<br><br>No que diz respeito ao CSAR, algumas autoridades da UE e organizações da sociedade civil alertaram que a proposta apresenta riscos à criptografia e os direitos fundamentais.<br><br>Os organismos de proteção de dados consideram que a proposta levanta "sérias preocupações em matéria de proteção de dados e privacidade" e apelaram por sua alteração, "em particular para garantir que as obrigações de detecção previstas cumprem as normas de necessidade e proporcionalidade aplicáveis e não resultam no enfraquecimento ou degradação da criptografia em um nível geral".[326]<br><br>Analisando as comunicações em torno da proposta, tais como a Avaliação de Impacto e as declarações públicas da Comissão Europeia, argumentou-se que a criptografia de ponta a ponta seria um fator que tornaria um serviço arriscado. Para mitigar o risco, os serviços podem sentir-se pressionados a remover a criptografia ou a aplicar a varredura pelo lado do cliente. Essa pressão será aplicada mesmo sem que os serviços estejam sujeitos a uma ordem de detecção.[327] |

321 Art. 1 do CSAR

322 Art. 2(f) do CSAR.

323 Considerando 13 do CSAR.

324 Art. 3(2)(b) do CSAR.

325 Partido Pirata Europeu, Lei dos Serviços Digitais: Decision in part strengthens, in part threatens privacy, safety and free speech online, 20 de janeiro de 2022, https://european-pirateparty.eu/eu-parliament-adopts-dsa-position/

326 Comitê Europeu para a Proteção de Dados e Autoridade Europeia para a Proteção de Dados (EDPB-EDPS), Parecer Conjunto 04/2022 sobre a Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras para prevenir e combater o abuso sexual infantil, 28 de julho de 2022, https://edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202204_csam_en_0.pdf

327 EDRi, Private and secure communications attacked by European Commission's latest proposal, 11 de maio de 2022, https://edri.org/our-work/private-and-secure-communications-put-at-risk-by-european-commissions-latest-proposal/

| | |
|---|---|
| Devem também considerar a forma como os usuários utilizam o serviço,[328] e como o provedor concebeu e opera o serviço.[329]<br><br>Quanto ao risco de aliciamento de crianças, devem considerar, por exemplo, funcionalidades como permitir que os usuários contatem outras pessoas diretamente e compartilhem imagens ou vídeos com elas, especialmente através de comunicações privadas.[330] Em seguida, os serviços devem tomar medidas para minimizar o risco identificado. Essas medidas devem ser eficazes, específicas e proporcionais e devem ser aplicadas de forma não discriminatória, tendo em devida conta as consequências para os direitos fundamentais.[331] Devem também reportar a avaliação de riscos e as medidas de mitigação à Autoridade Coordenadora nacional.[332] A Autoridade Coordenadora pode solicitar à autoridade judicial nacional competente que emita uma ordem de detecção sempre que exista um risco significativo de o serviço ser utilizado para abuso e os benefícios da emissão da ordem de detecção superem os riscos para os direitos de todas as partes envolvidas.[333] | Também foram levantadas preocupações quanto ao grau de independência do Centro da UE em relação à Europol e às autoridades policiais, com temores que a proposta, na prática, atribua um mandato de vigilância em massa a uma organização policial centralizada.[334]<br><br>Documentos internos sugerem que os Estados-membros da UE estão divididos.[335] A Áustria, por exemplo, votou uma resolução vinculativa para rejeitar a proposta da UE na sua forma atual, dado o risco de uma obrigação geral de monitoramento e como isso ameaça a criptografia e os direitos fundamentais.[336] |

328 Art. 3(2)(c) do CSAR

329 Art. 3(2)(d) do CSAR.

330 Art. 3(2)(e)(iii) do CSAR.

331 Art. 4(2) do CSAR.

332 Art. 5(1) do CSAR.

333 Art. 7(4) do CSAR.

334 Centre for Democracy and Technology (Europe Office), *Briefing on Key Concerns Relating to a Proposal for Regulation laying down the Rules to Prevent and Combat Child Sexual Abuse (CSAM)*, 26 de Maio de 2022, https://cdt.org/wp-content/uploads/2022/06/CDT-Europe-Briefing-on-Key-Issues-in-CSAM-Proposal.pdf

335 Patrick Breyer MEP, *Chat control: Internal documents show how divided the EU member states are*, 15 de Setembro de 2022, https://www.patrick-breyer.de/en/chat-control-internal-documents-show-how-divided-the-eu-member-states-are/

336 epicenter.works, *Chat control - a good day for privacy*, 3 de Novembro de 2022, https://epicenter.works/content/chatcontrol-a-good-day-for-privacy



| | |
|---|---|
| Os serviços que receberem ordens de detecção devem instalar e operar tecnologias que detectem abusos[337], as quais devem ser eficazes, suficientemente confiáveis, incapazes de extrair qualquer informação além da estritamente necessária e com o menor impacto possível na privacidade dos usuários, incluindo a confidencialidade da comunicação.[338]<br><br>O CSAR da UE também estabelece o Centro da UE sobre o Abuso Sexual de Crianças como uma entidade independente, embora dependa dos serviços de apoio da Europol. O Centro da UE tem uma série de tarefas, desde facilitar a geração e compartilhamento de conhecimentos e competências até atuar como um canal de denúncia dedicado para a UE e, em algumas circunstâncias, realizar pesquisas online para produção de material sobre abuso acessíveis ao público.[339] | |

337 Art. 10(1) do CSAR.

338 Art. 10(3) do CSAR.

339 Arts. 40-50 do CSAR.

# Uma abordagem dos direitos das crianças à criptografia: princípios para os formuladores de políticas

A concretização de toda a gama de direitos das crianças em ambientes digitais é complexa e cheia de nuances. Não existem soluções únicas para todos. Este relatório estabelece um conjunto de recomendações baseadas em princípios para regulações futuras de forma a respeitar os direitos das crianças.

Há desafios persistentes na defesa dos direitos de crianças à proteção contra a violência no ambiente digital, na detecção e denúncia de conteúdos e na ação contra perpetradores, assim como no apoio insuficiente e inconsistente do Estado na prevenção da violência contra crianças, na assistência às vítimas e aos sobreviventes e na cooperação transfronteiriça.

Quando houver interferência no comportamento e atividade das crianças num ambiente digital, incluindo o acesso a conteúdos digitais e/ou moderação de conteúdos, encriptados ou não, a lei deve ser aplicada num contexto e caso específicos, e o seu impacto avaliado tanto em termos de compreensão do panorama geral em escala quanto do incidente específico.

Compreender o funcionamento da criptografia e dos papéis que ela desempenha no ecossistema digital é essencial para uma regulação eficaz e que respeite direitos. Os diferentes propósitos da criptografia precisam ser compreendidos no contexto em que ela é usada no ambiente digital e de suas finalidades.

A criptografia não pode ser abordada isoladamente como uma questão de proteção das crianças, ou colocada em oposição à privacidade e segurança, mas deve ser vista como parte dos sistemas no ambiente digital. O próprio ambiente digital é parte do ecossistema social mais amplo. Nenhuma lei ou desenvolvimento tecnológico pode proteger crianças *online* ou garantir seus direitos humanos isoladamente. Cada parte do ecossistema social mais amplo requer tanto um nível adequado de investimento quanto o reconhecimento de suas limitações. Deve ser dada especial atenção à vasta gama de atores que se relacionam com as crianças na sociedade, incluindo autoridades de aplicação da lei, serviços de saúde e sociais, escolas e outras instituições, além do papel que cada um desses pode e deve desempenhar de forma eficaz e legítima, os seus limites e a necessidade de cooperação.

## Enquadramento e processo

1. **As ações que afetam o ambiente digital devem respeitar toda a gama de direitos das crianças.**

   Todas as intervenções que afetem o ambiente digital em geral, e as ações que envolvam a criptografia em particular, devem respeitar toda a gama de direitos das crianças, desde a proteção contra a violência até a privacidade e a liberdade de expressão.

   - **Privacidade *e* proteção:** As discussões devem ir além da dicotomia "privacidade versus proteção". Todos os envolvidos nos processos de tomada de decisão devem reconhecer que todos os direitos das crianças, incluindo a privacidade e a proteção, são universais, indivisíveis e interdependentes. Isto significa que esses direitos se aplicam a todas as crianças, em todos os lugares. Não existe um conjunto de direitos que seja mais importante que outros – todos os direitos são igualmente importantes. Esses direitos também se apoiam mutuamente, sendo o cumprimento de cada um necessário para a concretização dos outros.

   - **Avaliações de impacto aos direitos da criança:** Todas as intervenções que tenham um impacto significativo nas crianças devem basear-se em avaliações de impacto aos direitos de crianças. Isso deve envolver um escrutínio pré-legislativo que avalie o impacto de qualquer proposta de reforma legislativa em toda a gama de direitos deste grupo. Quando um órgão independente for responsável pela regulação, ele deve incluir conhecimentos suficientes sobre direitos de crianças. As empresas com um impacto significativo nos direitos deste grupo social neste contexto também devem realizar avaliações de impacto aos direitos das crianças, agir com base nos resultados dessas avaliações e apresentar relatórios sobre a sua implementação.

2. **As intervenções que envolvem a criptografia devem ser vistas dentro de um ecossistema mais amplo.**

   Nenhuma lei, política ou desenvolvimento tecnológico pode proteger as crianças online ou garantir os seus direitos humanos de forma mais ampla. A criptografia não pode ser abordada isoladamente, mas apenas como parte de um ecossistema mais amplo, com uma gama de intervenientes que podem interagir de forma significativa, cada um em seu próprio papel que pode ser desempenhado de forma eficaz e legítima.

   - **Comece pelo problema social:** A criptografia não deve ser o ponto de partida nos debates sobre problemas sociais que afetam as crianças. Em vez disso, os formuladores de políticas devem identificar o objetivo político a ser alcançado e considerar a gama de opções, de natureza tecnológica ou não, que poderiam ser implementadas para esse fim.



   Ao avaliar possíveis soluções, os formuladores de políticas devem considerar a variedade de atores que interagem no ecossistema social, incluindo agências governamentais, autoridades responsáveis pela aplicação da lei, serviços de saúde, serviços sociais, escolas, centros de cuidados e outras instituições.

   - **Cuidado com o tecnossolucionismo:** Os formuladores de políticas e outras partes interessadas devem evitar confiar em soluções tecnológicas únicas. A tomada de decisões deve basear-se numa compreensão profunda do complexo cenário tecnológico, incluindo, em particular, os múltiplos papéis que a criptografia e outras tecnologias desempenham. As políticas devem basear-se na capacidade razoável da tecnologia tal como ela é, e não como se poderia esperar que fosse.

   - **Apoie todo o ecossistema de proteção infantil:** Proteção infantil requer confiança humana e interação significativa por meio de infraestruturas sólidas para compartilhamento de conhecimentos e intervenção. Na medida em que já existam leis, políticas e outras iniciativas para efeitos de proteção da criança, elas devem ser totalmente implementadas. Deve haver uma ênfase na prevenção e na educação, e deve ser previsto financiamento adequado à vasta gama de serviços que interagem no ecossistema, desde a aplicação da lei e o sistema judicial, até os serviços sociais e de apoio às vítimas. Deve ser dada especial ênfase à formação de pessoal, que deve incluir, sempre que adequado, a gestão, a análise e a prática de provas digitais, a fim de promover a investigação e a persecução penal contra os autores de violência contra as crianças possibilitada pela tecnologia.

3. **Todos aqueles com conhecimentos relevantes devem estar envolvidos.**

   Todos os profissionais com conhecimentos relevantes devem ser capazes de participar de discussões e tomadas de decisões relativas a crianças e o ambiente digital, inclusive em matéria de criptografia. Devem poder fazê-lo em pé de igualdade e num ambiente de respeito mútuo. As conversas devem incluir especialistas que trabalham em proteção de crianças, tecnologia e regulação da Internet, proteção de dados e privacidade, bem como aqueles com conhecimentos mais generalistas em direitos das crianças, direitos humanos e direitos digitais. As opiniões da sociedade civil, da academia, do governo, das autoridades responsáveis pela aplicação da lei e do setor empresarial devem ser levadas em conta. Devem ser promovidos esforços especiais para incluir aqueles que trabalham fora dos espaços anglo-cêntricos e eurocêntricos atualmente dominantes.

   - **Linguagem:** Deve ser reconhecida a extrema sensibilidade dos aspectos do debate em torno da criptografia e dos direitos das crianças, particularmente no que diz respeito à exploração e abuso sexual infantil online. Os envolvidos nas discussões devem exercer empatia e prestar especial atenção ao enquadramento e à linguagem utilizados, bem como às expectativas que estão sendo criadas para vítimas e sobreviventes de abuso.

- **Dados:** Deve ser enfatizada a importância de dados precisos, em particular sobre a escala do abuso e a precisão das tecnologias de detecção de conteúdos. Todos os participantes nas discussões devem se esforçar para explicar extensivamente as formas como utilizam os dados para apoiar os seus argumentos, a fim de ajudar a sanar as diversas causas dos problemas e fazer avançar o debate sobre as soluções.

4. **As crianças e outras comunidades diretamente afetadas devem ser ouvidas e os seus pontos de vista devem ser devidamente considerados.**

   O direito das crianças a que as suas vozes sejam ouvidas e que lhes seja dada a devida importância deve ser defendido em todos os processos de tomada de decisão que lhes digam respeito. Outras comunidades diretamente afetadas, como as vítimas adultas e os sobreviventes da exploração e abuso sexual infantilou as que são desproporcionalmente afetadas pelo policiamento, pela vigilância, pela coleta de informações ou por outras práticas intrusivas em matéria de dados, também devem ser incluídas de forma significativa nestes processos. Não devem ser feitas suposições sobre os resultados que esses grupos podem desejar. Nem todas as crianças ou membros de uma comunidade têm as mesmas experiências, opiniões ou preocupações. Os processos de tomada de decisão devem, portanto, procurar incluir vozes diversas.

5. **Os formuladores de políticas envolvidos no tema da criptografia devem abordar o impacto para além da sua própria jurisdição.**

   O ambiente digital está interligado e é muito provável que a regulação numa jurisdição provoque efeitos em cascata em outras, ou mesmo a nível mundial. Os formuladores de políticas devem trabalhar para compreender essas ligações, inclusive se envolvendo em conversas com quem trabalha em diferentes jurisdições, especialmente com quem não faz parte dos debates anglo-cêntricos e eurocêntricos dominantes.

## Substância

6. **Não deve haver nenhuma proibição generalizada da criptografia para crianças.**

   Se a criptografia fosse removida de todos os serviços que as crianças utilizam, longe de as proteger, isso as deixaria vulneráveis a uma ampla gama de exploração e abuso. É possível regular as aplicações de criptografia, mas de forma consistente com os direitos das crianças.

7. **As intervenções que envolvem criptografia devem ser específicas ao contexto.**

   As medidas devem ser adaptadas às diversas experiências das crianças como titulares plenos de direitos, incluindo crianças de grupos desfavorecidos e marginalizados. As intervenções devem considerar e abordar contextos políticos, econômicos, sociais e culturais específicos e as diversas formas como as crianças se relacionam com o Estado, as empresas e as suas comunidades e famílias.



- **Usos do ambiente digital no mundo real:** Os envolvidos em tomadas de decisão devem promover uma melhor compreensão da variedade de utilizações do ambiente digital no mundo real, incluindo comunicações que envolvam informações médicas, organização política legítima em ambientes repressivos ou a dependência rotineira de determinadas plataformas onde há acessibilidade limitada a outros serviços. Devem ser empreendidos mais esforços para incluir perspectivas que não são necessariamente consistentes com as expectativas daqueles que vivem nos contextos anglo-cêntricos e eurocêntricos.

- **A reorientação da tecnologia:** Deve haver um reconhecimento de que as tecnologias para a detecção de conteúdos no ambiente digital podem ser reorientadas. A natureza do conteúdo que precisa ser identificado não é específica da tecnologia, mas específica da política. As ferramentas utilizadas para detectar conteúdos ilegais, como materiais de abuso sexual infantil, também podem ser utilizadas para identificar conteúdos legítimos e violar os direitos de quem os acessa.

8. **As medidas em relação à criptografia devem ser legais, necessárias e proporcionais.**

   As intervenções que envolvam a criptografia devem respeitar os princípios da legalidade, necessidade e proporcionalidade. Estes princípios aplicam-se ao conteúdo das comunicações, mas também à coleta, ao compartilhamento e à guarda de metadados. As medidas devem ser previstas em lei e devem ser suficientemente claras e precisas. Devem limitar-se a alcançar um objetivo político legítimo e devem ser a forma menos intrusiva de atingi-lo. As intervenções devem ser limitações necessárias e proporcionais aos direitos qualificados das crianças, como a privacidade, portanto devem ser dotadas de um elevado grau de especificidade, em vez de serem aplicadas indiscriminadamente.

9. **A elaboração de políticas deve abordar o papel das empresas**

   A regulação e a elaboração de políticas devem exigir mais transparência sobre a forma como as plataformas previnem e remediam as violações dos direitos das crianças, inclusive exigindo termos de serviço claros, acessíveis e adaptados às crianças. As plataformas devem receber orientação sobre como melhorar a concepção dos serviços, especialmente sobre ferramentas de denúncias de usuários voltadas para crianças. As empresas cujas atividades tenham um impacto significativo nos direitos das crianças devem ser incentivadas a investir na pesquisa, no desenvolvimento e no compartilhamento de resultados sobre novas tecnologias, bem como no apoio aos esforços de outros que trabalham nesta área.

   - **Denúncia às autoridades:** Quando as empresas obtiverem conhecimento da existência, nos seus serviços, de conteúdo ilegal, como material de abuso sexual infantil, ou atividade ilegal, como violência contra crianças, devem tomar medidas de acordo com os seus termos de serviço e rapidamente denunciar o ocorrido às autoridades policiais ou outras autoridades competentes.

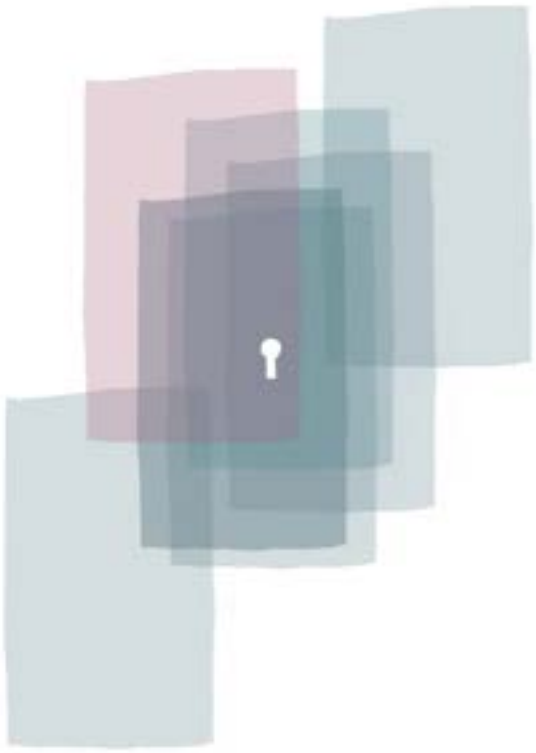
- **Transparência:** As empresas devem publicar relatórios de transparência sobre a escala da exploração e abuso sexual infantil *online* nos seus serviços que cheguem ao seu conhecimento, detalhando os tipos de conteúdo e comportamento identificados e as ações tomadas em consequência. Devem ser feitos esforços para alcançar o máximo de especificidade possível, desmembrando os eventos em casos individuais de abuso, analisando a prevalência da vitimização por meio do compartilhamento de conteúdos idênticos ou alterados, e indicando o contexto em que os eventos ocorreram, se for relevante para determinar a intenção dos usuários envolvidos (por exemplo, compartilhamento consensual de imagens entre crianças ou conteúdo compartilhado de forma ofensiva).

**10. As crianças devem ter acesso à justiça.**

Devem existir mecanismos de reclamação gratuitos, eficazes e adaptados às crianças, tanto judiciais como extrajudiciais, para garantir que as crianças tenham acesso a soluções, em tempo útil para as violações de toda a sua gama de direitos no ambiente digital. Deve haver mecanismos de supervisão independentes para garantir que medidas que envolvam criptografia tenham uma implementação legal e que respeite direitos.

- **Denúncia pelos usuários:** Devem ser disponibilizadas ferramentas de denúncia para usuários que sejam confidenciais, seguras e adequadas para crianças, a fim de garantir que as crianças possam denunciar materiais e comportamentos nos serviços que utilizam e buscar ação. Também devem ser considerados mecanismos de "sinalizador confiável". A decisão após a denúncia dos usuários deve ser tomada tempestivamente e deve basear-se num processo claro e transparente, dando aos usuários a possibilidade de acessar mecanismos de recurso. Devem ser produzidos relatórios de transparência para permitir a fiscalização das políticas e práticas sistêmicas em torno da denúncia dos usuários, protegendo ao mesmo tempo os direitos dos usuários, das vítimas e dos sobreviventes.

- **Precisão na detecção de conteúdo:** A dependência excessiva de ferramentas automatizadas acarreta o risco de erros no processo de detecção e remoção indevida de conteúdo, bem como outras possíveis consequências negativas, como o banimento de contas de usuários. A automação pode apoiar, mas não pode substituir a moderação humana de conteúdo. Quaisquer resultados inadvertidos devido a erros de processos automatizados devem ser reversíveis por meio de suporte humano.



CRIN CHILD RIGHTS INTERNATIONAL NETWORK

defend|digital|me

ip.rec Instituto de Pesquisa em Direito & Tecnologia do Recife