



# ENCRYPTION THE GUARDIAN

MONDAY, OCTOBER 21ST 14.30 UTC

## Global Encryption Day – October 21 2024 - Encrypt Today to Safeguard Tomorrow: The Encryption Summit

### Criptografia, a Guardiã

**Sharayah Lane - Internet Society:** Obrigado a todos por se juntarem a nós no painel de hoje, The Guardian. Hoje vamos falar sobre criptografia e os impactos que a criptografia tem na segurança das crianças online. Meu nome é Sharayah Lane. Sou Conselheira Sênior na Internet Society e também membro da nossa equipe de criptografia.

Grande parte do meu trabalho com a equipe de criptografia tem se concentrado na segurança infantil online, e esta é uma área relativamente nova que muitos de nós estamos explorando. Será uma boa discussão hoje. Temos alguns palestrantes maravilhosos. Quando se trata do tema da criptografia e da segurança das crianças online, a discussão tem se concentrado principalmente nos perpetradores de abusos e exploração de crianças na internet.

O que não ouvimos tanto, no entanto, é o papel que a criptografia desempenha em manter as crianças seguras online. Hoje vamos abordar esse tema com nosso painel de especialistas. Nossos palestrantes trabalham em áreas que se concentram no uso seguro da Internet por crianças. Eles são acadêmicos que conduzem pesquisas na área, e o objetivo da sessão de hoje é que nossos participantes tenham uma melhor compreensão de como a criptografia desempenha um papel em manter as crianças

seguras online, para apoiar cada um de vocês, nossos participantes, a serem melhores defensores da criptografia com mais informações para adicionar às suas próprias áreas de trabalho.

E além da conversa de hoje, três dos nossos painelistas também contribuíram para um documento de um grupo de trabalho colaborativo que aprofunda mais nesse tópico. Se você estiver interessado em ler esse artigo, você pode encontrá-lo aqui, e eu vou postar isso no chat para que você possa encontrar o artigo aqui se estiver interessado em ler mais.

Mas primeiro vou apresentar nossos painelistas. Primeiro, temos Jessica Dickinson Goodman. Jessica conecta os mundos da tecnologia e da política. Ela atuou como presidente do conselho da Internet Society da área da Baía de São Francisco, apoiando o trabalho excepcional de sua equipe em políticas de tecnologia, educação e ajudando comunidades carentes a obter melhor acesso à Internet. Ela também é autora do livro de 2023, "Criptografia para Bebês".

Em seguida, temos Larry Magid. Larry é Doutor em Educação e também CEO do ConnectSafely.org. Ele é um jornalista veterano de tecnologia. Escreve uma coluna semanal para o San Jose Mercury News e é o apresentador do ConnectSafely Report, transmitido duas vezes por semana pela CBS News Radio nos EUA. Ele é frequentemente convidado em programas de TV e rádio nacionais e locais, tanto nos EUA quanto no Reino Unido. Serviu por 20 anos como analista de tecnologia no ar para a CBS News e é o apresentador do popular programa da CBS, Eye on Tech.

Em seguida, temos a Dra. Sabine Witting. A Dra. Witting é professora assistente de direito e tecnologias digitais na Universidade de Leiden. Sua pesquisa foca na interseção dos direitos humanos, incluindo os direitos das crianças, com a tecnologia digital. Ela também é cofundadora da TechLegality, uma empresa de consultoria especializada em direitos humanos e tecnologias digitais. Sabine é pesquisadora não residente no Center for Democracy and Technology.

Em seguida, temos o Dr. Ezequiel Passeron. O Dr. Passeron possui doutorado em Educação e Sociedade pela Universidade de Barcelona e é graduado em Ciências da Comunicação pela Universidade de Buenos Aires. Ele também possui um mestrado em Ambientes de Ensino e Aprendizagem Mediados por Tecnologias Digitais. Ele é da Universidade de Barcelona. Ele é o Diretor de Educomunicação na Faro Digital, uma ONG que estuda e desenvolve projetos em alfabetização midiática. Também é Professor Associado na Universidade de Barcelona, Coordenador da Rede Conectados ao CERN e Pesquisador no Grupo de Pesquisa ESBINA. Seus interesses estão no estudo e análise das interseções entre educação, comunicação, plataformas digitais e ambientes de inteligência artificial.

Por último, temos o Dr. Mark Leiser. Dr. Leiser é um teórico regulatório especializado em regulação digital, legal e de plataformas. Seu foco está na lei e nas tecnologias

digitais, como direitos fundamentais, comércio eletrônico, teoria regulatória, regulação de plataformas, contratos, segurança, privacidade, liberdade de expressão, cibercrime e fenômenos relacionados ao design enganoso, Padrões Enganosos, Proteção ao Consumidor e o Uso e Regulação de IA e Tecnologias Digitais. Então, temos muita expertise na chamada de hoje. Muito obrigado a todos por estarem conosco e compartilharem seu tempo e conhecimento sobre o tema. Agradecemos muito. Com isso, vamos começar nossa sessão de perguntas e respostas.

Vamos fazer algumas perguntas específicas para nossos palestrantes. Incentivamos todos os nossos participantes a enviarem suas perguntas também, usando a função de perguntas e respostas. Teremos um tempo no final da nossa chamada de hoje para abordar suas perguntas e levá-las aos palestrantes.

Mas com isso, vamos começar nossa conversa e iniciaremos com Larry Magid. Então, Larry, você tem trabalhado bastante no espaço de engajamento online de crianças. Você pode nos dar uma visão geral sobre o que aprendeu sobre como a criptografia desempenha um papel no uso da Internet pelos jovens?

**Larry Magid - ConnectSafely.org:** Obrigado. Primeiro, quero reconhecer que há, sem dúvida, um grande número de pessoas bem-intencionadas que argumentam que a criptografia é necessária para que as autoridades impeçam a exploração de crianças, e estão pensando especificamente no CSAM, material de abuso sexual infantil.

Há controvérsia dentro da comunidade de proteção infantil, e francamente acho que a maioria dos meus amigos e colegas dessa comunidade discordaria de mim. E argumentariam que a necessidade de prevenir o CSAM, com a qual obviamente concordo, mas que a necessidade das autoridades, que a criptografia atrapalha e, portanto, causa danos.

E isso provavelmente torna o trabalho da aplicação da lei mais difícil. Todas as questões têm certos tipos de nuances e compensações, e de forma alguma quero, de qualquer maneira, diminuir a importância do bloqueio e prevenção de CSAM, a chamada pornografia infantil, de material de abuso sexual infantil, bem como a perseguição daqueles que traficam de uma maneira que prejudica e abusa das crianças.

Dito isso, também é importante destacar que as próprias crianças precisam de proteção contra possíveis violações de privacidade e segurança que podem ocorrer em um mundo sem criptografia. Há muitos exemplos, desde vazamentos de dados onde informações de crianças caíram nas mãos de criminosos ou potenciais criminosos, até situações em que suas informações foram simplesmente reveladas de maneiras que violam sua privacidade.

Pode-se até argumentar que a criptografia protege as crianças contra predadores infantis, pois a capacidade de acessar informações sobre crianças facilita para aqueles

que querem abusar delas encontrá-las, alcançá-las e explorá-las. Portanto, isso é uma faca de dois gumes.

Mas eu, ao pensar muito sobre isso, acredito que, claramente, a capacidade de proteger a privacidade e a segurança das crianças é um direito fundamental que deve ser mantido. E as autoridades precisam encontrar outras maneiras dentro do regime de um mundo criptografado para poder cumprir sua responsabilidade de combater o material de abuso sexual infantil.

Mas há muitos exemplos onde, novamente, mencionei vazamentos de dados, então lembro que o Serviço Nacional de Saúde no Reino Unido teve um grande vazamento há alguns anos com informações sobre crianças. Há muitos casos de dados escolares sendo violados e há muitos casos de crianças se comunicando diretamente com outras pessoas de uma maneira que poderia ter sido violada ou talvez tenha sido violada como resultado da falta de uma plataforma criptografada.

Então, eu realmente acho que todos nós merecemos proteção. Seja em bancos e transações financeiras, seja para ativistas em vários países, e, a propósito, crianças podem estar entre os ativistas. Quando pensamos em pessoas envolvidas em atividades que os governos querem suprimir, em muitos casos, são menores de idade que estão engajados, adolescentes, certamente, que estão envolvidos em atividades ao redor do mundo, onde ter a capacidade de manter comunicações privadas e confidenciais é essencial não apenas para sua missão de tentar reformar as coisas, mas também para a proteção de suas próprias vidas, porque muitas vezes há um grande perigo associado a fazer parte de um movimento, independentemente da sua idade.

E há tantos exemplos que precisamos destacar. E acho que o que estou tentando fazer dentro da comunidade em que atuo é levar as pessoas a pensarem além do simples desejo das forças da lei de proteger, mas na questão mais ampla de proteger toda a nossa segurança e privacidade. E, finalmente, e isso não foi um pensamento original meu, mas de um dos meus colegas que ajudou a trabalhar neste documento que você mencionou anteriormente, ele destacou que a criptografia pode muitas vezes ser usada para ajudar a detectar e processar crimes, mas, desculpe, a falta de criptografia pode tornar mais fácil processar crimes, mas a criptografia ajuda a prevenir crimes.

E, dada a escolha entre processar e prevenir, eu escolheria a prevenção todas as vezes. Seria ótimo acabar com o trabalho dos promotores porque eliminamos o crime. Provavelmente nunca conseguiremos isso. Mas se pudermos reduzir o crime protegendo a segurança das pessoas, isso significa menos casos para os promotores perseguirem.

**Sharayah Lane - Internet Society:** Isso é ótimo. Obrigado, Larry. E eu queria passar para a Jessica. Sei que a Jessica vai ter que sair da chamada mais cedo, então obrigado por estar conosco. E minha pergunta para você é: o que te motivou a escrever o livro

"Criptografia para Bebês"? Qual era a sua esperança de que os leitores levassem consigo após terminar de ler o livro?

**Jessica Dickinson Goodman - SF Bay ISOC:** Tenho interesse em criptografia desde que fiz estágio na Electronic Frontier Foundation quando estava no ensino médio, porque sou esse tipo de pessoa e esse tipo de nerd. Mas na época, eu estava em casa com meu filho, que fará dois anos em três semanas. E eu estava lendo muitos livros para ele sobre coisas como astrofísica para bebês.

Há uma série de livros de bordo que muitas crianças pequenas têm nos Estados Unidos, com estatísticas para bebês e astrofísica para bebês. E eu queria explicar criptografia para ele. Achei que seria um desafio interessante e ele é um garoto esperto. E, e sempre é complexo, certo? Como você explica algo que não é físico, que é técnico?

Mas eu imaginei que, se pudéssemos ler astrofísica para bebês, poderíamos encontrar uma maneira de falar sobre criptografia. Então, quando escrevi e testei com ele, e depois pedi aos meus amigos para testarem com seus filhos, e depois fiz um evento pop-up no centro de Mountain View, passei sete horas pedindo a cada pessoa técnica que passava para tentar desafiar as metáforas que usei, e eles não encontraram erros técnicos, o que foi maravilhoso.

E depois colocá-lo à venda online para beneficiar meu capítulo em San Francisco, meu principal objetivo era ajudar tanto as crianças quanto os pais que estão lendo para elas a se sentirem mais confortáveis com a criptografia. Às vezes, quando você diz que se importa com a criptografia, como eu atualmente em Georgetown fazendo pós-graduação na Escola de Serviço Estrangeiro, desejei a todos um feliz Dia Global da Criptografia para aqueles que celebram.

E nem todo mundo se sentirá imediatamente confortável com a ideia. Agora há um estigma associado ao desejo de manter a privacidade de seus filhos em alguns espaços, como o Sr. Vedgett estava falando, particularmente na área em que ambos trabalhamos no Vale do Silício, onde existe uma narrativa muito forte da aplicação da lei em torno de tentar facilitar seus trabalhos de acusação.

E eu costumava trabalhar para o Departamento de Justiça da Califórnia. Eu me importo com esse trabalho também. Mas esta é uma ferramenta essencial para os pais poderem manter sua família segura, e entendê-la bem o suficiente para explicá-la a uma criança pequena é valioso, em vez de enfrentar a onda de táticas de medo, tentando dar aos pais uma corda para sair de toda essa pressão para serem contra a criptografia.

Porque eu acho que é uma coisa boa querer proteger a localização, a privacidade e as fotos do seu filho. E eu posso entrar em detalhes técnicos com outros adultos, mas meu

filho não precisa saber sobre todas essas partes. Vou dizer, eu não tinha certeza se ia incluir a frase E2EE no livro, e é a parte favorita do meu pequeno.

Ele diz, E2EE! Ele acha muito divertido dizer essa parte e me pede para repetir várias vezes. Então, às vezes podemos ser um pouco técnicos, mesmo com nosso público mais jovem, e eles conseguirão nos acompanhar, pelo menos se for divertido de dizer em voz alta.

**Sharayah Lane - Internet Society:** Adoro isso. Adoro essa história. E também estou ansiosa para conferir o livro.

Tenho um pequeno que está mais ou menos na mesma idade, então isso será divertido. Antes de você sair, Jessica, queria te fazer mais uma pergunta enquanto ainda temos você aqui. Você trabalhou extensivamente no papel da criptografia na proteção dos direitos reprodutivos das mulheres nos EUA. Pode compartilhar mais sobre esse trabalho e como isso se conecta à segurança das crianças através da criptografia?

**Jessica Dickinson Goodman - SF Bay ISOC:** Absolutamente. Após o vazamento da decisão Dobbs, fui ao meu conselho. Para aqueles que não estão familiarizados, a maioria dos capítulos é inteiramente baseada em voluntários, então começamos a conversar. Sabíamos que era um tópico sensível, mas queríamos capacitar as pessoas com informações para manter seus dados seguros. Durante todo o ano em que a decisão Dobbs foi vazada e quando foi divulgada, nosso capítulo realizou mensalmente o que eu chamo de treinamentos de suporte técnico tático, abertos a qualquer pessoa no mundo.

Acho que tínhamos meia dúzia de países representados. Muitas pessoas de estados como o Texas, onde o governo está ativamente buscando coletar informações privadas. E nos concentramos em dois estudos de caso. Um era de uma jovem que estava tentando buscar cuidados para aborto no Texas e precisava sair e reunir essas informações sem, como tem sido o caso, ser processada por um parceiro ou presa pela polícia, ou ter seus amigos ou familiares processados, presos ou multados, o que é atualmente a lei em vigor que está sendo contestada no Texas e que muitas pessoas que buscam cuidados para aborto estão enfrentando.

O outro estudo de caso foi de uma jovem que estava no Alabama e que estava buscando cuidados de confirmação de gênero fora do estado e tinha uma preocupação em casa. Então, esses são os dois estudos de caso. Cuidados de saúde reprodutiva onde você tem uma preocupação com o estado bisbilhotando suas informações e usando-as contra você. E o outro era a preocupação com membros da família bisbilhotando e potencialmente sendo violentos por causa dessas informações.

Então, trabalhamos para entender quais são as questões logísticas, quais são as ferramentas técnicas. Muito disso foi inspirado por ser uma pessoa queer, uma mãe e uma mulher. E eu preciso dessas ferramentas. Para que eu possa ser livre no mundo da

mesma forma que as pessoas sem úteros são livres no mundo, e da mesma forma que as pessoas heterossexuais são livres no mundo, e eu preciso ter privacidade porque meu governo, embora eu aspire a trabalhar para ele algum dia e já tenha trabalhado para ele no passado, não representa todos os americanos, não apenas os americanos que concordam comigo e que querem que eu esteja segura e feliz.

E essa série de treinamentos foi importante para mim, importante para o nosso capítulo e importante para as pessoas que participaram, porque guiou as pessoas sobre como configurar o WhatsApp, como usar o Tor Browser, o que é isso? E a maioria das perguntas surgia desse medo que o Sr. Magic mencionou, de que as pessoas não tinham certeza se essas ferramentas eram para elas.

E se essas ferramentas eram seguras para eles usarem. E assim que conversamos sobre isso, a maioria das pessoas se sentiu confortável em seguir em frente e usar mais ferramentas de criptografia. Mas acho que lembrar que as pessoas no governo são apenas pessoas e membros da família são apenas famílias e eles vão ser bons e maus e feios e maravilhosos, assim como qualquer outra pessoa, e eles não merecem acesso especial à localização.

imagens ou comunicações, eles podem obter um mandado, assim como fariam há cem anos, e obter essas informações. Eles não precisam de acesso especial só porque é 2024. Então, foi isso que fizemos e as informações de treinamento ainda estão online. A Electronic Frontier Foundation tem uma estrutura maravilhosa de autodefesa digital que usamos.

Também usamos o site Plan C para encontrar informações sobre cuidados com o aborto, o que foi importante e está se tornando ainda mais importante à medida que mais estados aprovam leis para criminalizar o acesso a cuidados de afirmação de gênero e saúde reprodutiva.

**Sharayah Lane - Internet Society:** Obrigado por isso, e obrigado por todo o excelente trabalho que você faz.

Vou passar para Sabine. E obrigado por estar conosco hoje. Você ocupou um cargo na ONU trabalhando na Namíbia e no Zimbábue em questões de reforma de leis e políticas sobre cibercrime, responsabilidade do setor privado e tecnologias digitais. Quais foram algumas das principais descobertas que surgiram para você nesse trabalho em relação à segurança das crianças online e, ou com o papel da criptografia?

**Dr Sabine K Witting - Leiden University:** Sim, muito obrigada. Obrigada por me receberem. Então, como eu estava dizendo, trabalhei especificamente com a UNICEF por muitos anos na África Austral, mas também na região do Leste Asiático e Pacífico. E uma coisa que está surgindo em muitos países do Sul Global é a conectividade e o acesso às tecnologias digitais.

E claro que isso também significa maior acesso e conectividade para as crianças. E por mais que as tecnologias digitais possam ser muito úteis para que as crianças realizem seus direitos, é claro que também existem certos riscos para os direitos das crianças. E, particularmente, acho que o que recebe mais atenção é o direito à proteção contra todas as formas de violência, abuso e exploração.

E eu acho que quando estamos, quando estávamos trabalhando nesses tópicos aqui na região, uma das coisas que sempre lembrávamos aos legisladores e formuladores de políticas era dizer: olhem, claro, é um tópico emergente que parece algo novo, mas as dinâmicas subjacentes dessas formas de violência, abuso e exploração são exatamente as mesmas que vimos no ambiente físico.

Então, quando você pensa em como prevenir e responder a esse tipo de ofensa, precisa realmente pensar de forma mais ampla e não apenas no espaço digital, mas realmente considerar todo o sistema de proteção infantil e como fortalecer esses sistemas de proteção para também poder responder a esses casos facilitados pela tecnologia.

Portanto, reconhecer essa conexão entre a violência física e a facilitada pela tecnologia foi realmente muito importante para desenvolver uma abordagem holística e não recorrer ao solucionismo técnico, algo que ainda vemos muito, não apenas no Sul Global, mas também no Norte Global.

Então, acho que da mesma forma, quando estamos discutindo esse tipo de intervenções políticas e olhando especificamente para o lado da aplicação da lei. Certamente há também uma falta de valorização da comunicação privada e da criptografia. E acho que isso ocorre porque não valorizamos da mesma forma a privacidade e a segurança na comunicação para as crianças.

Simplesmente não parece ser algo que esteja na mente das pessoas. Claro que a proteção contra a violência é muito importante, mas ao mesmo tempo, precisamos realmente pensar em todo o espectro dos direitos das crianças. E acho que uma das coisas que foi realmente bastante reveladora para mim foi quando estávamos trabalhando com crianças no Zimbábue no desenvolvimento da Política de Proteção Online da Criança do Zimbábue.

Perguntamos às crianças: qual é a sua experiência online? Quais são as coisas que vocês encontram? E houve, claro, muitas crianças que disseram que experimentaram várias formas de violência, incluindo violência sexual. Mas também houve crianças que nos disseram que estavam usando um VPN para manter sua segurança. E quando trouxemos esses achados de volta aos legisladores em Harare, você podia ver que muitas pessoas na sala, os legisladores, não sabiam o que era um VPN.

E eu acho que este é um aspecto bastante interessante do debate: as experiências das crianças e o foco das crianças no que é importante para elas em relação às tecnologias

digitais muitas vezes diferem do que os adultos acham realmente importante. E também vimos isso na região do Sul da Ásia, onde perguntamos às crianças o que elas querem das empresas de tecnologia para tornar os produtos e serviços digitais mais adequados para elas.

E novamente, na lista de desejos, bem no topo da lista de desejos, estava mais proteção de dados e privacidade. E então eu acho que isso é Para nós e realmente para legisladores e formuladores de políticas um bom chamado à ação em termos de consultar as crianças, não apenas sobre a declaração do problema. Então, até que ponto você experimenta A, B, C, D, mas também o que você acha das soluções que estamos propondo?

E acho que é aqui que as vozes das crianças estão muito ausentes e, na verdade, não apenas as vozes das crianças, mas as vozes de todos os grupos vulneráveis que são afetados pela criptografia, como Jessica mencionou. Mulheres, pessoas queer, mas também defensores dos direitos humanos, todos teriam seus direitos consideravelmente diminuídos.

E acho que isso é algo em que simplesmente não estamos realmente levando em consideração as opiniões das pessoas afetadas, o que também inclui as crianças. Obrigado.

**Sharayah Lane - Internet Society:** Obrigado. E sim, continuaremos essa conversa um pouco mais tarde. Com Larry, porque sei que o Connect Safely tem um Conselho Consultivo de Jovens sobre o qual eu adoraria saber mais.

Mas primeiro, quero ouvir todos os nossos palestrantes, e depois voltaremos a fazer perguntas variadas para cada um deles. A próxima pergunta é para Ezequiel. E isso, na verdade, continua um pouco a partir da pergunta de Sabine. Sua organização trabalha significativamente com jovens e suas famílias.

O que os pais geralmente fazem e não percebem que pode estar expondo seus filhos? O que eles podem fazer melhor? E qual é o papel da criptografia em tudo isso?

**Ezequiel Passeron - University of Barcelona:** Ótimo. Muito obrigado, antes de mais nada, pela oportunidade de compartilhar com essas pessoas maravilhosas.

Acho que temos que celebrar esses espaços para ter tempo e diálogo.

Acho que o primeiro problema que vemos nas famílias é a falta de diálogo intergeracional. Na Argentina e na América do Sul, crianças e jovens estão muito sozinhos no mundo digital. Seus adultos desconhecem suas práticas e cultura digital. Então, quando surge um problema, eles não são as pessoas a quem os jovens recorrem para dialogar.

Em Faro, os principais problemas que estamos vendo quando conversamos e ouvimos os alunos, crianças e jovens são a violência digital, a desinformação e a má informação, uma personalização crescente da experiência, as bolhas de filtro, a falta de contexto com a diferença, todos os problemas que essas coisas estão causando para a convivência social e a democracia, e também a hipersexualização e a monetização dos imaginários e subjetividades dos jovens. É por isso que na nossa ONG promovemos momentos de conexão que incentivam o diálogo, conversas, tentando não julgar sobre temas que interessam aos jovens para entender o cuidado que eles precisam, acho que o cuidado é um grande conceito que temos que colocar em primeiro plano. Além disso, práticas adultas como, não sei, a parentalidade, por exemplo, surgem. Que é compartilhar imagens pessoais de crianças e jovens e eles veem que é um grande problema e não gostam disso.

Muitas crianças estão começando a ter uma identidade digital sem sequer terem consentido. Em relação ao papel da criptografia, acreditamos que é uma grande aliada para as famílias, pois é algo geralmente desconhecido em nosso país. Estudamos o guia de criptografia da ISOC que você acabou de compartilhar e vemos uma grande oportunidade de entregá-lo nas escolas.

Achamos que esse tipo de ferramentas, adicionadas a oficinas educacionais e, novamente, tendo tempo e espaço para dialogar e construir reflexão, poderiam ser uma abordagem integral para alcançar esses aliados-chave na proteção e cuidado dos jovens. A família frequentemente fala sobre controles parentais, senhas ou tempo de tela seguro.

Como Sabine disse anteriormente, queremos um botão para resolver todos os nossos problemas. E pensamos que a criptografia poderia ser uma técnica muito boa para colocar acima dos cuidados que precisamos ter. Com crianças e jovens.

**Sharayah Lane - Internet Society:** Sim, obrigado. É muito interessante essa mudança de dinâmica que aconteceu, até mesmo com coisas como a regulamentação.

Então, sempre foi responsabilidade dos adultos manter as crianças seguras em várias áreas. Mas quando se trata de espaços online e de tecnologia, muitas vezes os jovens são mais informados, conhecedores e experientes do que alguns dos mais velhos. Isso realmente muda a conversa e a dinâmica de como realizar esse trabalho.

Sim, isso é realmente importante. Vou passar para o Mark para a nossa próxima pergunta. Mais um lembrete, se vocês, participantes da audiência, tiverem perguntas, por favor, coloquem-nas na função de perguntas e respostas. Já recebemos algumas e vamos respondê-las em alguns minutos, então continuem enviando suas perguntas para nossos palestrantes e teremos tempo para respondê-las.

A academia desempenha um papel importante na pesquisa e no estudo de como as crianças interagem online. Quais têm sido algumas das principais descobertas de sua pesquisa ao longo dos anos em relação à criptografia?

**Dr Mark Leiser - Digital, Internet, and Platform Regulation:** Então, talvez eu vá trapacear um pouco e começar com uma ótima pergunta que surgiu na sessão de perguntas e respostas, que na verdade vou acabar respondendo em parte na minha própria resposta a essa pergunta, então só queria destacar isso.

Eu diria que, ao longo dos anos, houve inúmeros incidentes em que a criptografia proporcionou segurança às crianças em suas interações digitais, mas também houve uma lacuna na compreensão de sua importância, o que as deixa vulneráveis. Nas pesquisas que realizei, e obviamente o Dr. Witting também, descobrimos que plataformas não criptografadas expõem as crianças a riscos. Desde rastreamento de localização, metadados, até cyberbullying em aplicativos de mensagens não protegidos. Em contraste, o uso de sistemas criptografados reduz drasticamente essas ameaças. Por exemplo, um caso envolvendo uma criança que compartilhou sua localização sem saber através de uma postagem em rede social, levando estranhos a aparecerem em sua casa.

E esse incidente, e outros semelhantes, destacam como a criptografia pode servir como um escudo, protegendo os dados sensíveis que não queremos que caiam em mãos erradas. Mas, crianças e pais ainda carecem de educação para reconhecer seu valor, o que os torna suscetíveis a ameaças digitais. E a micro narrativa é tentar olhar para esses incidentes específicos onde a criptografia teria mantido uma criança segura em um determinado contexto.

Mas, em uma escala mais ampla, a integração da criptografia em plataformas, escolas e ambientes de jogos teve um impacto substancialmente positivo na segurança infantil. A criptografia impede o acesso não autorizado a dados pessoais. Ela reduz o roubo de identidade. Diminui o cyberbullying e o stalking, e durante a pandemia, a mudança para o aprendizado online ressaltou ainda mais a importância da criptografia.

Quando as escolas passaram a usar sistemas de videoconferência criptografados, isso mitigou riscos como o Zoom bomb e as intrusões digitais em salas de aula virtuais. Ainda há uma lacuna na conscientização sobre o papel da criptografia na proteção das crianças online. Como já foi dito antes, a pesquisa e a política devem convergir para abordar essas vulnerabilidades, promovendo a criptografia e expandindo sua implementação em plataformas frequentadas por crianças.

E, finalmente, essa espécie de mega narrativa é que a criptografia está ligada aos princípios fundamentais de privacidade e segurança. E tem implicações profundas para os direitos e liberdades digitais. Enquanto o GDPR da UE incentiva fortemente a criptografia como um método de proteção de dados pessoais, o cenário global mostra diferenças marcantes em como a criptografia é realmente tratada.

Em regimes autoritários, restrições à criptografia permitem a vigilância em massa, o que compromete a privacidade e os direitos humanos. E a relação entre privacidade e segurança torna-se inegável. Não são duas coisas separadas, são dois lados da mesma moeda. A criptografia mantém as pessoas seguras. Ela serve como um pilar fundamental para proteger indivíduos, especialmente crianças e outros membros vulneráveis da sociedade, da exploração e do dano que os pais estão tão desesperados para evitar para seus filhos.

À medida que as sociedades se tornam mais dependentes desse tipo de infraestrutura digital, leis como o GDPR e outras que promovem a proteção de dados e a privacidade por design são realmente vitais para garantir a segurança e a dignidade das populações vulneráveis em todo o mundo. Obrigado.

**Sharayah Lane - Internet Society:** Uau, essa foi uma excelente visão geral.

Obrigado, Mark. E obrigado por responder a uma de nossas perguntas. Temos outras chegando. Então, novamente, um lembrete para nossos participantes: sintam-se à vontade para digitar suas perguntas aos palestrantes na função de Perguntas e Respostas, e teremos tempo para respondê-las um pouco mais tarde em nossa chamada. Nossa próxima pergunta é para Larry, e isso pode esclarecer um pouco do que temos falado sobre incluir os jovens na conversa e, em última análise, na solução.

Então, o ConnectSafely tem um Conselho Consultivo de Jovens Adultos. Como trabalhar diretamente com os jovens influenciou seu trabalho, e quais são algumas das principais coisas que você está ouvindo deles agora?

**Larry Magid - ConnectSafely.org:** Ter um conselho consultivo de jovens realmente nos fundamenta de muitas maneiras, e nos ensina algumas das coisas que os jovens almejam, além de nos mostrar algumas preocupações deles. Tenho que dizer que, em algumas áreas, os jovens são um pouco mais conservadores do que eu em relação a certas questões.

Às vezes, me surpreende o quanto eles estão preocupados com tantos perigos na Internet e como estão ansiosos para ver mais controles implementados. Não tivemos conversas extensas sobre criptografia. Planejamos fazer isso no futuro como parte da nossa agenda, mas imagino que teríamos uma diferença de opinião.

Isso parece ser uma das coisas que você aprende conversando com pessoas de qualquer demografia: você não pode rotular nenhuma demografia, seja por gênero, raça, orientação sexual, idade ou qualquer outra coisa. As pessoas são pessoas com opiniões diferentes. Mas, em geral, acho que certamente alguns dos jovens com quem conversei têm um desejo muito forte de ver uma Internet que seja segura e privada e realmente entendem a necessidade de criptografia de maneiras semelhantes às que Mark mencionou e outros, como uma forma de protegê-los de possíveis abusos online.

Há outros que podem estar preocupados com as limitações ou os desafios que isso impõe à aplicação da lei, e isso é algo que faria parte de um programa educacional para tentar fazer com que as pessoas compreendam melhor por que a criptografia é tão importante e como a aplicação da lei ainda pode fazer seu trabalho, apesar de ter ferramentas, assim como fazem seu trabalho apesar das várias proteções legais que existem nos Estados Unidos e em outros países não autoritários, na medida em que os Estados Unidos, esperamos, continuem sendo um país não autoritário.

Mas sim, é muito importante para nós, no mundo das políticas, estarmos conversando com os jovens. E, novamente, sem fazer suposições sobre o que eles possam dizer, mas dando-lhes um lugar à mesa. Na verdade, este ano, como parte do Connect Safely, somos os anfitriões do Dia da Internet Segura nos EUA.

E este ano vamos ter uma conversa sobre políticas em Sacramento, o governo estadual onde fica a capital da Califórnia, para tentar proporcionar aos jovens um papel na mesa de discussões, para que quando os legisladores estiverem aprovando leis, seja sobre criptografia, controle parental, verificação de idade, redes sociais, ou suposta anti-dependência, ou qualquer outra coisa, os jovens façam parte dessa conversa.

Queremos ver um aumento no número. Gostaríamos de ver mais educação para os jovens sobre criptografia. Uma das razões pelas quais a Connect Safely fez vários artigos e teve a honra de ser a anfitriã do documento que este grupo elaborou é porque queremos garantir que cada vez mais jovens entendam a criptografia.

Minha percepção é que, para a maioria das pessoas, é um assunto que elas realmente não abordaram. Portanto, há uma necessidade urgente de ter muitas conversas educativas com pessoas de todas as idades, mas especialmente com adolescentes.

**Sharayah Lane - Internet Society:** Sim, obrigado. E compartilhei um link para o Dia da Internet Segura no chat, caso alguém esteja interessado em saber mais.

**Larry Magid - ConnectSafely.org:** Ah, a propósito, estamos oferecendo subsídios este ano, como fizemos nos últimos anos, para educadores e organizações sem fins lucrativos. Então, se alguém quiser fazer um programa sobre criptografia em sua comunidade ou em suas escolas, temos subsídios de até 1.000 para professores e organizações sem fins lucrativos para ajudá-los a realizar educação comunitária no Dia da Internet Segura, que será em fevereiro próximo.

Então, por favor, verifique novamente em algumas semanas quando as inscrições serão lançadas.

**Sharayah Lane - Internet Society:** Sim, obrigado por esse recurso. É uma ótima maneira de dar continuidade à chamada de hoje também. Então, com isso, eu queria

passar a palavra para Ezequiel para continuar essa conversa, porque Ezequiel, você também trabalha muito de perto com crianças, jovens e suas famílias.

E espero poder fazer a grande pergunta e abordar o elefante na sala: materiais de abuso sexual infantil, materiais CSAM. Também vi um comentário sobre isso no chat. Então, como protegemos contra isso? E o que há nessa caixa de ferramentas? E qual é parte do trabalho que vocês têm feito na FonoDigital sobre isso?

**Ezequiel Passeron - University of Barcelona (2):** Como eu disse antes, a hipersexualização da sociedade, mas também das crianças, é um assunto importante que precisamos enfrentar, e a maneira como interagimos com as plataformas digitais tem algo a ver com isso. Não acreditamos na determinação dos meios de comunicação de massa sobre nossas práticas, mas eles têm uma forte influência, sem dúvida.

Na Argentina, temos um trabalho significativo sendo realizado por promotores especializados em crimes cibernéticos. Sabemos que há uma extensa cooperação internacional, especialmente com a rede NMAC, que facilita a troca de informações sobre casos e o progresso das investigações em cada instância. O fato é que esse tipo de caso, chamamos em espanhol, masi, temos o tempo todo essa concepção errada de pornografia infantil.

É material de exploração sexual infantil e temos que. Temos que falar alto para entender o grande problema. Está surgindo cada vez mais. Temos muitos casos de crianças e escolas que não sabem como, o que fazer. Então, há um papel fundamental aí para envolver os promotores.

E delegacias de polícia que estão trabalhando nesse tipo de casos. Também estamos vendo em nossos workshops que tecnologias como IA estão sendo usadas para gerar imagens de crianças que violam seus direitos e privacidades. Na semana passada, tivemos um caso recente que estava no topo das notícias e da mídia.

E como podemos nos proteger disso? E com quais ferramentas? Acho que essas são as perguntas-chave que devemos fazer. Mais uma vez, enfatizamos a educação, a cidadania digital e a criação de espaços de diálogo. Acho que esse tipo de questão sexual é, às vezes, um pouco tabu em nossas sociedades.

Mas quando as crianças estão na Internet e entre plataformas digitais, não há tabu. Aprendemos fazendo. E na maioria das vezes, antes de termos um espaço para questionar, descobrimos nossa sexualidade com nossos pais ou com um adulto de confiança. Acreditamos que a educação, o diálogo e a criação de espaços seguros para que as crianças possam expressar suas curiosidades e todas as coisas que precisam aprender passo a passo são as principais coisas que devemos promover e defender.

**Sharayah Lane - Internet Society:** Sim, e realmente há muitas maneiras diferentes de olhar para isso. Não há uma resposta clara e acho que isso está realmente no cerne da nossa discussão de hoje, que é abordar a questão de que, quando se trata de criptografia e do impacto na segurança das crianças online, grande parte do foco tem sido nos perpetradores de abuso e nos adultos e na comunidade.

as implicações da criptografia para os jovens online se perdem nessa conversa. Então, como manter uma proteção para os jovens online através da criptografia enquanto se processa e aborda a questão dos materiais de abuso sexual infantil é uma questão em aberto no momento, e é algo em que muitas pessoas estão trabalhando e refletindo.

E realmente é um dos grandes desafios do momento, porque como ouvimos de nossos palestrantes antes, o número de maneiras que a criptografia desempenha um papel para os jovens. Então, simplesmente removê-la também tem um efeito. Então, obrigado por um pouco mais de contexto sobre isso. Sei que essa é sempre uma questão difícil.

E Sabine, eu queria voltar para você. Você tem trabalhado extensivamente aconselhando formuladores de políticas ao redor do mundo sobre tecnologia. Qual é uma das principais coisas que você aconselha os formuladores de políticas quando se trata da segurança das crianças online?

**Dr Sabine K Witting - Leiden University:** Sim, e muito obrigado por essa pergunta. Claro, sempre partimos de uma perspectiva de direitos humanos e direitos das crianças.

Nosso principal conselho é que não podemos isolar a segurança das crianças e seu direito à proteção dos outros direitos das crianças. E, conforme a Convenção das Nações Unidas sobre os Direitos da Criança, todos esses diferentes direitos das crianças são interdependentes, indivisíveis e inter-relacionados.

Isso significa que não podemos avançar em um direito sem considerar o impacto adverso ou os impactos positivos de outros direitos na convenção. E como isso se traduz em termos de aconselhamento, o que os legisladores devem fazer concretamente quando estão em uma situação em que pensam sobre leis e políticas.

O primeiro passo para a segurança online das crianças é realmente realizar uma avaliação de impacto sobre os direitos humanos, incluindo um foco específico nos direitos das crianças. E o que isso significa é realmente usar a metodologia proposta pelos Princípios Orientadores da ONU sobre Empresas e Direitos Humanos, na verdade, para pensar, ok, quais são os direitos humanos afetados em geral, não apenas para adultos, mas especificamente para populações vulneráveis e crianças.

E então um segundo passo é pensar, ok, até que ponto. Até que ponto esses direitos são impactados? Qual é a escala? Qual é o alcance em várias jurisdições? E acho que

isso é uma das coisas que sempre destacamos, que mesmo se você for a UE e estiver considerando políticas que impactam a criptografia de ponta a ponta, deve saber que isso tem um impacto nas leis e políticas em todo o mundo.

E como você disse, trabalhamos nessas decisões políticas em todo o mundo, e não posso te dizer quantas vezes vimos disposições, por exemplo, do Ato de Segurança Online do Reino Unido, copiadas e coladas em novas leis de cibersegurança onde o contexto obviamente é muito diferente em países onde o estado de direito pode não ser igualmente respeitado, e isso é, claro, uma grande preocupação.

Então, uma vez que essa avaliação de impacto sobre os direitos humanos tenha sido feita, precisamos realmente pensar sobre, ok, que medida podemos agora implementar que considere todos esses diferentes direitos afetados? E é aqui que o termo proporcionalidade se torna importante, e acho que quando olhamos para os debates em torno da segurança infantil e da criptografia de ponta a ponta.

Todos afirmam que suas medidas são proporcionais. E o que me impressiona é que as pessoas parecem pensar que a proporcionalidade não tem realmente uma metodologia. É apenas algo que você sente, se uma coisa ou outra é mais importante, então você simplesmente alega a proporcionalidade dessa medida específica.

E eu acho, claro, vindo de, eu sou da Alemanha, e trabalho muito na UE, e damos muita ênfase à metodologia por trás dos testes de proporcionalidade. E há duas coisas que eu gostaria de destacar. A primeira é perguntar: essa medida é realmente necessária? Temos alguma medida igualmente eficaz, mas menos intrusiva?

E somente quando tivermos esgotado essas medidas, então podemos pensar em medidas mais intrusivas. E acho que quando estamos pensando em medidas menos intrusivas, como essas abordagens sistemáticas para fortalecer o sistema de proteção infantil, ainda estamos falhando consideravelmente em todos os aspectos. Se você olhar para algumas avaliações dos sistemas de proteção infantil também em países do Norte global.

A narrativa é quase sempre a mesma. Não temos assistentes sociais suficientes. Não temos agentes da lei especializados nessas questões. Os professores não são treinados. Os médicos não são treinados para identificar casos de abuso e exploração. Então, minha pergunta é, mesmo que conseguíssemos detectar todas essas imagens de abuso sexual infantil, quem vai responder a isso?

Então, a resposta provavelmente é ninguém, porque ainda não temos um sistema de proteção infantil suficientemente equipado. E acho que é aqui que realmente precisamos pensar se essa medida é realmente a melhor maneira de abordar esse problema. E o segundo ponto é sobre a proporcionalidade, o teste de proporcionalidade em si, onde um dos primeiros passos é realmente avaliar, ok, até

que ponto um direito específico é afetado. E esse nível de violação tem uma linha vermelha, e isso é o que chamamos de essência do direito.

E uma vez que alcançamos essa essência de um direito específico, então essa é uma linha vermelha. E então não importa realmente o que está do outro lado da balança, por assim dizer, esse direito é infringido. não pode ser infringido. E essa linha vermelha, eu acho, é algo que realmente precisamos considerar quando falamos sobre abolir ou enfraquecer a criptografia de ponta a ponta no contexto das comunicações privadas, porque eu argumentaria que essa linha vermelha provavelmente já foi alcançada.

Acho que isso não é discutido suficientemente e precisamos realmente voltar aos fundamentos da lei dos direitos humanos e avaliar de uma perspectiva holística o que essa medida significa para os direitos humanos e os direitos das crianças em geral. Obrigado.

**Sharayah Lane - Internet Society:** Não, obrigado.

E obrigado por mencionar a convenção de ter uma maneira de medir. Algo contra o qual medir é realmente útil e eu li a convenção sobre os direitos das crianças e acho que há muitas coisas ali que são relevantes e que se alinham diretamente com a criptografia e as crianças terem acesso à criptografia online.

Mas, novamente, é uma conversa contínua, então eu queria passar para o Mark. Você fez uma quantidade significativa de pesquisa sobre o lado legal da tecnologia. Existem atualmente leis que apoiam a criptografia que deveríamos conhecer? Se sim, qual poderia ser o impacto delas? Se não, por que você acha que isso acontece?

**Dr Mark Leiser - Digital, Internet, and Platform Regulation:** Existem poucas leis que realmente dizem que você deve ter, não acho que haja nenhuma lei como a Lei de Criptografia ou algo assim, mas temos várias leis que, na prática, apoiam a criptografia. Como acadêmico europeu trabalhando ao lado do Dr. Witting, na Holanda e no Reino Unido.

O RGPD obviamente tem uma espécie de lei fundamental de privacidade de dados, proteção de dados para a UE com efeito extraterritorial e alguns podem até argumentar o efeito Bruxelas, em que outros países têm que adotar para cumprir nossas regras e ter acesso ao nosso mercado.

Existem duas ou três coisas diferentes nisso. Primeiro, a obrigação do Artigo 25 de proteção de dados desde a concepção e por padrão. Então, se você está desenvolvendo uma tecnologia onde poderia proteger dados, ou precisa proteger dados, então ao integrar a criptografia na fase inicial não é uma obrigação obrigatória, mas ajuda as empresas a pensarem nos riscos e a tomarem medidas para garantir que os dados estejam seguros e protegidos.

Agora, por que isso é importante? Porque, de acordo com o Artigo 32, os controladores e processadores de dados são obrigados a implementar medidas técnicas e organizacionais adequadas para proteger os dados pessoais. E uma das coisas destacadas para garantir a segurança dos dados é a criptografia. Agora, qual é o impacto disso? O impacto é que, sob o GDPR, se os dados criptografados forem comprometidos em uma violação, mas permanecerem inacessíveis devido à criptografia forte, as penalidades para a empresa podem ser significativamente reduzidas.

Então, isso se torna um grande incentivo para as empresas implementarem protocolos de criptografia. O segundo ponto é que, como mencionei anteriormente, o GDPR tem um efeito cascata nas leis de privacidade e proteção de dados ao redor do mundo. Muitas empresas, mesmo aquelas fora da UE, adotam a criptografia como uma prática recomendada para conformidade.

Gigantes globais da tecnologia como Apple, WhatsApp e Google adotaram a criptografia de ponta a ponta em parte para se alinhar aos padrões do GDPR. E a criptografia de ponta a ponta do WhatsApp garante que apenas as partes comunicantes, em teoria, possam ler as mensagens, impedindo até mesmo a própria empresa de acessar o conteúdo.

Agora, nos EUA, a CCPA, a Lei de Privacidade do Consumidor da Califórnia, que é frequentemente vista como o equivalente americano ao GDPR, enfatiza a importância de proteger os dados pessoais. Então, não é obrigatório, mas é tratado como um fator atenuante ao avaliar penalidades por violações de dados, assim como o GDPR. Se uma empresa sofrer uma violação, mas puder provar que os dados comprometidos estavam criptografados, a responsabilidade e os danos podem ser reduzidos. A CCPA tem, na verdade, se tornado um catalisador para leis de privacidade federais e estaduais.

Se você construir leis no modelo do CCPA, incorporar a criptografia se torna uma medida de segurança recomendada. A lei um tanto desconhecida sobre privacidade e proteção de dados na UE é a Diretiva de Privacidade Eletrônica. E isso é frequentemente referido como a lei dos cookies. E isso governa a confidencialidade das comunicações dentro da UE.

A ideia aqui é que essa lei e a regulamentação proposta que a substituirá devem fortalecer o papel da criptografia para garantir a confidencialidade das comunicações eletrônicas. Essas leis, por si só, você pode ir ao Brasil e ver a criptografia como uma prática de segurança padrão para empresas que operam no Brasil.

Isso ajuda a criptografia a mostrar que eles estão em conformidade com a LGPD e também a se manterem competitivos nos mercados globais. E então você tem outras especificidades setoriais, como a HIPAA nos EUA, a Lei de Portabilidade e Responsabilidade de Seguro de Saúde. Novamente, ela não exige criptografia, mas

fornece aos provedores de saúde, planos de saúde e seus associados comerciais a implementação de salvaguardas técnicas para proteger as informações de saúde.

Portanto, é uma salvaguarda endereçável, o que significa que, embora não seja obrigatório, deve ser implementado ou documentado por que uma medida alternativa é suficiente. Então, mesmo os regulamentos como o HIPAA, a expansão da criptografia na tecnologia da saúde, à medida que estamos construindo sistemas inteiros para o compartilhamento de dados de saúde de um provedor para outro, para trabalhar com médicos, hospitais, companhias de seguros e afins para transferir dados de saúde de forma contínua e sem interrupções, a criptografia é vista como a ferramenta para proteger a privacidade dessas comunicações.

Há algumas na emenda da legislação de telecomunicações e outras da Austrália sob o Ato de Assistência e Acesso. Há outro exemplo de tentativa de obrigar a criptografia. O último ponto é por que não há mais leis obrigando a criptografia? Então, em algumas áreas, isso se resume a equilibrar a segurança nacional e a privacidade.

Mencionamos isso na minha discussão anterior. Os governos hesitam em obrigar o uso de criptografia porque isso poderia interferir nas operações de aplicação da lei e de segurança nacional. Em outros países em desenvolvimento, parece que a infraestrutura legal para apoiar a criptografia ainda não evoluiu completamente, e assim você não tem leis de privacidade em vigor, e por isso a criptografia nem sempre tem sido priorizada.

E o terceiro é a pressão real de regimes autoritários. Assim, a criptografia é vista como uma ferramenta que pode permitir a dissidência, enfraquecendo o controle estatal sobre a informação. Como resultado, alguns regimes estão ativamente desencorajando o uso da criptografia ou impondo restrições legais a ela. Então, você pode ver a dicotomia entre privacidade e segurança e autoritarismo versus democracia.

E acho que sei de que lado quero estar e vou deixar por isso mesmo. Muito obrigado.

**Sharayah Lane - Internet Society:** Sim, obrigado por essa visão geral. E acho que provavelmente continuaremos parte dessa conversa em nosso próximo painel, pois será um tópico importante. E o que é tão interessante sobre o lado legal da criptografia é que você vê uma diferença tão grande onde, em alguns lugares, estão trabalhando para proteger legalmente esse direito à privacidade e em alguns países estão trabalhando para dismantelar totalmente.

E é interessante ver que há uma diferença tão grande entre os dois e observar essas diferentes tendências ao redor do mundo. Essa é uma parte importante do nosso trabalho de defesa no ISOC: analisar as leis de criptografia ou leis que enfraqueceriam a criptografia ao redor do mundo e realizar trabalho de defesa em escala global.

Então, isso foi uma ótima visão geral. Obrigado por isso. Acho que temos tempo para mais uma. Vou fazer nossa pergunta individual antes de passarmos para a sessão de perguntas e respostas. Última chance, vamos entrar na parte de perguntas e respostas, então, se você tiver perguntas para nossos palestrantes, por favor, coloque-as na função de perguntas e respostas no Zoom, que fica ao lado do botão de chat e do botão de participantes na sua tela.

Última pergunta, eu queria voltar para Ezequiel. E eu queria perguntar, qual é algo importante, e vou dizer algo porque tenho certeza de que há muitas coisas, mas qual é algo importante que você aprendeu ao iniciar uma organização como a Faro Digital sobre as experiências dos jovens online e como podemos trabalhar para proporcionar melhores experiências para eles no futuro?

**Ezequiel Passeron - University of Barcelona (2):** Ótimo. Obrigado pela última pergunta. Nos últimos anos, devido à economia da atenção e ao modo como as plataformas operam, temos notado um crescente interesse e uma forte influência na subjetividade dos jovens em relação ao que chamamos de monetização. Isso se refere à busca de gratificação e recompensas em cada ação, uma característica comum de qualquer rede social.

Isso cria uma dinâmica onde a Internet ou o espaço digital é percebido como uma fonte de renda a partir de casa, aparentemente sem muito esforço. Práticas como jogos de azar online, onde os adultos estão muito preocupados, mas quando vamos a workshops e ouvimos os jovens, eles não veem isso como uma concepção vergonhosa.

Então, há uma grande lacuna que precisamos preencher. A venda de imagens íntimas, os investimentos surgiram na Argentina. Uma regulamentação foi implementada há algumas semanas, permitindo que indivíduos com mais de 13 anos entrem no mercado financeiro. E essa regulamentação não é algo isolado. Obrigado.

Isso, isso se refere a uma prática que eles têm em suas atividades online. Então, o que vemos como um problema ou mais como um desafio é a questão da confiança. O que os leva a cair vítimas de golpes digitais, por exemplo. Na Argentina, falamos sobre Poncidemia, um problema que é alimentado pelo surgimento desses jovens influenciadores que eles chamam de Poncipros.

Eles estão o tempo todo dizendo, cara, você tem que investir nisso, você tem que fazer esse curso, são supostos influenciadores que incentivam outros jovens a se tornarem seus próprios chefes, terem tempo livre, ganharem muito dinheiro todo mês de seus sofás. Claro que são os velhos esquemas Ponzi que existiam antes da Internet, mas que agora encontraram nas plataformas digitais veículos para recrutar e atrair mais pessoas, especialmente em contextos economicamente desfavorecidos.

No mundo digital, vivemos em um território onde nossa atenção é explorada, onde nossas emoções e desejos estão no centro dos negócios das grandes empresas de

tecnologia. É por isso que precisamos criar, é por isso que falo sobre criar tempo e espaços, apenas entre parênteses, gostamos de pensar nisso como uma metáfora.

Precisamos proteger, precisamos cuidar, precisamos criar esses espaços onde crianças e jovens possam se desenvolver junto com os outros. Onde eles possam estudar e praticar assuntos mundiais sem um objetivo, uma meta ou utilidade. Apenas tentando entender o mundo e renová-lo, como Hannah Arendt nos disse há meio século.

Nosso tempo é o tempo desse grande problema, Wilson. CODIS, temos emoções paleolíticas, instituições de Maya Deedle e tecnologias divinas. Adoramos essa frase. Achamos que estamos em um momento em que precisamos recuperar o sentido da frase de Descartes, Cogito Ergo Sum. Quando pensamos nessa frase, a traduzimos como, Penso, logo existo.

Mas quando estudamos a etimologia da palavra cogito, descobrimos que ela se refere tanto a "eu penso" quanto a "eu cuido". Então, deixo uma pergunta para você. Quem são os responsáveis pela prática do cuidado em nossa sociedade? Acho que há uma questão revolucionária enorme e rebelde que precisamos lutar e defender para colocar os cuidados em outro lugar em nossa sociedade.

Obrigado.

**Sharayah Lane - Internet Society:** Não, isso é um excelente lembrete de que grande parte do desafio ou do problema está na maneira como o estamos encarando. E a forma como estamos abordando as coisas, acho que muito do que temos feito até agora tem sido a partir de uma perspectiva e compreensão desatualizadas, e a necessidade de realmente pensar profundamente sobre essas questões e entender o que os jovens estão enfrentando e passando, e dedicar tempo para compreender isso.

Todas essas coisas são tão importantes em nossa conversa mais ampla. Obrigado por trazer à tona o lado filosófico disso, porque acho que é uma peça que falta. Uma peça que falta na conversa. Então, vamos, temos apenas alguns minutos restantes. Vamos entrar na nossa sessão de perguntas e respostas do público.

Tenho uma pergunta traduzida aqui. Diz, eu, e isso é para qualquer um dos palestrantes, então sintam-se à vontade para responder. Achei interessante a criptografia de imagens de crianças. Como um fator de proteção contra o uso de imagens desse perfil de usuário ou não usuário, dependendo da idade da criança, a criptografia poderia ser usada para buscar, selecionar e remover imagens de crianças que não têm autonomia para expressar sua vontade?

**Larry Magid - ConnectSafely.org:** Certamente poderia ser usado para ocultar essas imagens e garantir que não sejam compartilhadas sem o consentimento da criança ou de seus responsáveis. Não tenho certeza se poderia ser usado de forma independente

para procurá-las. Talvez alguns dos especialistas mais técnicos tenham uma resposta para isso.

Mas certamente pode proteger a privacidade dessas imagens, garantindo que elas cheguem apenas às pessoas com quem se pretende compartilhá-las.

**Sharayah Lane - Internet Society:** Sim, então, como uma espécie de medida retroativa, ou voltando e removendo e escondendo imagens, não acredito que a criptografia possa ser usada como esse tipo de ferramenta, mas é mais uma característica preventiva, então evitaria. Obrigado. Obrigado. O uso não autorizado de imagens desde o início, mas se,

**Larry Magid - ConnectSafely.org:** se houver, pelo menos nos Estados Unidos, uma imagem sexualmente explícita de uma criança online, você pode ir, eu acredito que seja [takeitdown.org](http://takeitdown.org),

org, é um serviço da NECMEC, e removê-la. Existem vários sites que ajudam a combater a pornografia de vingança e outras distribuições de imagens íntimas de adultos também. Então, há ferramentas que você pode usar para removê-las, mas eu não acredito, como você disse, que você possa criptografá-las retroativamente.

**Sharayah Lane - Internet Society:** Certo, e estou pegando o link para esse recurso. Vou colocá-lo no chat também. E com isso, sei que acredito que o Mark respondeu um pouco sobre isso em sua resposta, mas também vou colocar essa questão para todo o grupo. Quando se trata de legislação e políticas sobre a segurança online das crianças, há uma tendência de propostas de cima para baixo, em vez de medidas que poderiam capacitar os pais a tomar decisões informadas sobre as atividades online de seus filhos.

Por exemplo, uma proposta é restringir legalmente os menores de usarem redes sociais após certos horários. Existe um equilíbrio entre as regras impostas pelo governo, como as leis de privacidade de dados nos EUA, e o empoderamento dos pais? E diz, sintá-se à vontade para desafiar completamente a minha formulação.

**Dr Mark Leiser - Digital, Internet, and Platform Regulation:** Posso acrescentar à minha resposta?

**Sharayah Lane - Internet Society:** Sim.

**Dr Mark Leiser - Digital, Internet, and Platform Regulation:** Sabina também levantou a mão. Tenho certeza de que ela tem algo a dizer sobre isso. Acho importante que os pais percebam que as crianças também têm direito à privacidade em relação aos pais. E que muitas vezes falamos sobre isso como algo que queremos dar aos pais para terem mais controle.

Mas também acho que precisamos reconhecer que a nova norma deve ser que as crianças tenham um espaço seguro para se comunicar, livre dos pais. E vou dar alguns exemplos rapidamente para reforçar esse ponto. O primeiro é que existem muitas culturas onde ser LGBT é desaprovado dentro de casa.

E se você vai explorar sua sexualidade, sua identidade sexual, você quer poder falar livremente, sem que seus pais bisbilhotem e olhem suas comunicações. O segundo, e mais óbvio para pessoas em culturas ocidentais, eu acho, especialmente nos dias de hoje, são as pessoas que estão procurando informações sobre saúde sexual e sua identidade.

E então, o terceiro é realmente proteger a criança de comunicações que possam ser prejudiciais, indesejadas ou não solicitadas. Se você lhes der um espaço seguro para se comunicarem, a criança estará capacitada para manter outras crianças afastadas. Essa é minha adição à questão, mas acho que também é importante reconhecer que os pais precisam oferecer à criança um espaço seguro onde ela possa se comunicar livremente, sem a supervisão dos pais.

E tenho certeza de que Sabina também terá outras opiniões sobre isso.

**Dr Sabine K Witting - Leiden University:** Sim, obrigado, Sabine. Sim, muito obrigado. Acho que o Mark também abordou esse ponto. Acho que quando sempre focamos nos pais, dizemos que não devemos infringir a criptografia. Devemos focar na alfabetização digital e no papel dos pais.

E eu concordo com isso. E acho que, até certo ponto, há um equívoco em pensar que os pais sempre agem no melhor interesse da criança. E acho que isso certamente não é o caso. E Mark mencionou alguns exemplos onde isso realmente pode não ser o caso, então colocar os pais no comando não necessariamente tornará a criança mais segura, e acho que isso é algo a se considerar.

E também acho que, neste debate, há um pouco de, é uma, há um foco ou na criptografia de ponta a ponta ou na alfabetização digital, e é como se usássemos uma ou outra medida. E acho que isso acaba deixando as empresas de tecnologia fora do gancho um pouco rápido demais. Porque, mesmo que não queiramos que elas criem brechas ou contornem essa criptografia de ponta a ponta, queremos que as empresas de tecnologia criem um ambiente seguro.

Para crianças, e isso deve ser feito através de esforços legislativos. Mark e eu escrevemos um capítulo de livro sobre isso, que acho que será lançado no próximo ano, onde analisamos o Ato de Serviços Digitais, por exemplo, e os tipos de medidas que o Ato de Serviços Digitais impõe aos intermediários para criar ativamente um ambiente seguro para as crianças, como a obrigatoriedade de relatar material ilegal, criar mecanismos de denúncia amigáveis para crianças e notificações.

E assim por diante. Então, eu acho que certamente há um grande papel para a alfabetização digital, mas não devemos colocar toda a responsabilidade nos pais ou nas crianças e simplesmente deixar as empresas de tecnologia fora de questão. Obrigado.

**Sharayah Lane - Internet Society:** Sim, eu concordo. Obrigado. E Larry.

**Larry Magid - ConnectSafely.org:** Sim, isso varia de país para país, mas nos Estados Unidos, há uma, eu não diria um consenso, mas a cultura é construída em torno da ideia de que os pais controlam seus filhos e todos os direitos de uma criança realmente passam pelos pais, enquanto os europeus têm uma atitude um pouco diferente, eu acho, e o fato é que, como Mark disse corretamente, as crianças precisam de um certo grau de autonomia, mesmo em relação aos próprios pais, e não apenas pelos motivos que Mark especificou, e todos eles eram muito bons, que um pai pode realmente ter uma atitude diferente em relação à saúde reprodutiva, identidade de gênero, orientação sexual, etc.

Mas também, nem todos os pais se sentem à vontade ou estão preparados para lidar com autoridades, e até mesmo as empresas de mídia social podem ser vistas como uma autoridade. Eles podem ter preocupações com a imigração, achando que, ao se envolverem em algo online para seus filhos, podem aumentar a possibilidade de terem problemas com as autoridades de imigração.

Eles podem não ter a alfabetização, seja a alfabetização técnica ou a alfabetização linguística. Eles podem não estar cientes, e há crianças que, infelizmente, têm pais que estão de outra forma despreparados, talvez por questões de saúde mental, ou simplesmente pelo fato de que suas vidas são muito caóticas ou ocupadas, etc.

Nem todas as crianças são atendidas por seus pais e nem todos os pais estão preparados para fornecer o tipo de apoio e estrutura de permissão que algumas dessas leis exigem deles. Então, eu me preocupo com as crianças sendo deixadas para trás por vários motivos, e isso antes de qualquer uma dessas leis ser aprovada.

Precisamos pensar nas consequências não intencionais.

**Sharayah Lane - Internet Society:** Sim, é muito importante. Quero agradecer a todos por estarem conosco hoje. Temos cerca de 6 minutos restantes juntos e, ao encerrarmos, gostaria de pedir a cada um dos nossos palestrantes um pensamento final, uma frase ou duas sobre o papel da criptografia na segurança das crianças.

Então, a pergunta para você é: por que a criptografia é importante para você quando se trata da segurança das crianças online? E podemos começar com o Mark.

**Dr Mark Leiser - Digital, Internet, and Platform Regulation:** Eu diria que, em uma ou duas frases, no nível social, privacidade e segurança não são apenas interligadas, mas

pilares que se reforçam mutuamente. Obrigado. Em uma democracia funcional, quando as crianças se sentem empoderadas e seguras, sabendo que suas informações pessoais não vão causar-lhes danos, isso contribui para um senso mais amplo de segurança infantil e confiança tanto no ambiente digital quanto no físico.

E ao enfraquecer as proteções de privacidade, pode-se levar a uma perda de segurança. E eu acho que quando você prioriza a privacidade e a segurança da criança, você garante a proteção de seus direitos, suas liberdades civis e sua confiança nas tecnologias digitais.

**Sharayah Lane - Internet Society:** Uau, isso é bom. Ezequiel, vamos passar para você.

**Ezequiel Passeron - University of Barcelona:** É complicado falar depois do Mark.

Obrigado por isso. Sim, eu acho que, por um lado, realmente precisamos fazer perguntas mais amplas, como Sabine nos disse antes, sempre tentamos pensar em uma solução técnica para os problemas que temos em nosso relacionamento com as técnicas. Eu acho que a natureza humana é técnica, certo?

Sem uma linguagem compartilhada, não podemos nos entender aqui. Por isso, achamos que precisamos começar a descobrir novas maneiras, caminhos e técnicas para salvaguardar nossos direitos primários. Eu acho que o empoderamento de crianças e jovens é vital. Realmente acredito que essa metáfora criada em 2001 dos Nativos Digitais surgiu como um grande problema para nós, adultos, cuidarmos das crianças, porque pensamos que elas sabem tudo sobre o mundo digital e que não podemos ajudá-las.

Eu realmente acredito que a criptografia é uma maneira segura de se empoderar em um território onde temos muitas empresas tentando fazer negócios com nosso tempo e atenção. E eu realmente acho que esse tipo de técnica pode salvar nossos direitos e criar ambientes poderosos para vivermos e aproveitarmos, sem sermos explorados. Acho que é isso, em poucas palavras.

**Sharayah Lane - Internet Society:** Sim, isso é ótimo. Obrigado. Sabine?

**Dr Sabine K Witting - Leiden University:** Sim, eu acho que se continuarmos a polarizar a discussão como está no momento, estaremos criando uma distração perfeita para os dois interessados que realmente deveriam investir em prevenção e resposta, que são os governos, investindo de verdade no sistema de proteção infantil, mas também as empresas de tecnologia, criando produtos seguros e que respeitem os direitos.

Então, acho que meu apelo seria realmente dar um passo atrás e perguntar Cui Bono, e isso certamente inclui governos e empresas de tecnologia. Obrigado.

**Sharayah Lane - Internet Society:** Isso é muito importante. Obrigado. E por último, Larry.

**Larry Magid - ConnectSafely.org:** Acho que todas as pessoas, independentemente da idade, têm direito à privacidade e segurança e ao direito de ter comunicações que sejam apenas entre elas e outras pessoas.

E eu acho que, depois de ouvir os palestrantes e pensar sobre nosso papel, precisamos mudar a abordagem. Sobre essa noção de proteção infantil e não permitir que as pessoas pensem que a proteção infantil é simplesmente capacitar as forças da lei, dando-lhes todas as ferramentas e ferramentas de vigilância de que precisam, mas também proteger as pessoas de criminosos, de membros da família, se necessário, e conhecidos, de governos que possam oprimi-los.

Ou simplesmente porque querem ter comunicações privadas. E, por fim, acho que precisamos redobrar nossos esforços na educação. Isso realmente me faz pensar, ao refletir sobre o Dia da Internet Segura e o trabalho que o ConnectSafely está fazendo com adolescentes, que todos nós precisamos fornecer aos adolescentes, e às crianças, todos os recursos possíveis para ajudá-los a proteger sua privacidade e segurança.

E isso além de todas as coisas que continuamos a fazer em relação a phishing e senhas, e também ensinamos a usar criptografia robusta como uma forma de se protegerem.

**Sharayah Lane - Internet Society:** Sim, mais uma vez, muito obrigado a todos. Tivemos uma riqueza de expertise e conhecimento na chamada de hoje, então realmente agradeço a vocês por dedicarem tempo para compartilhar conosco hoje.

Temos alguns ótimos recursos no chat, então sinta-se à vontade para seguir qualquer um dos links compartilhados hoje. Esperamos que vocês possam participar da nossa próxima sessão, que começará em cerca de 10 minutos, chamada "Criptografia Detida: a prisão de Pavel Durov do Telegram por não registrar serviços criptografados".

Então, novamente, isso parece ser um pouco de um seguimento à nossa conversa legal sobre criptografia e lei hoje. Portanto, se você quiser fazer uma pausa, terá cerca de 10 minutos antes da nossa próxima sessão para o Dia Global da Criptografia, mas obrigado aos nossos palestrantes e obrigado a todos os nossos participantes por se juntarem a nós hoje.

Tudo bem. Obrigado. Tchau.