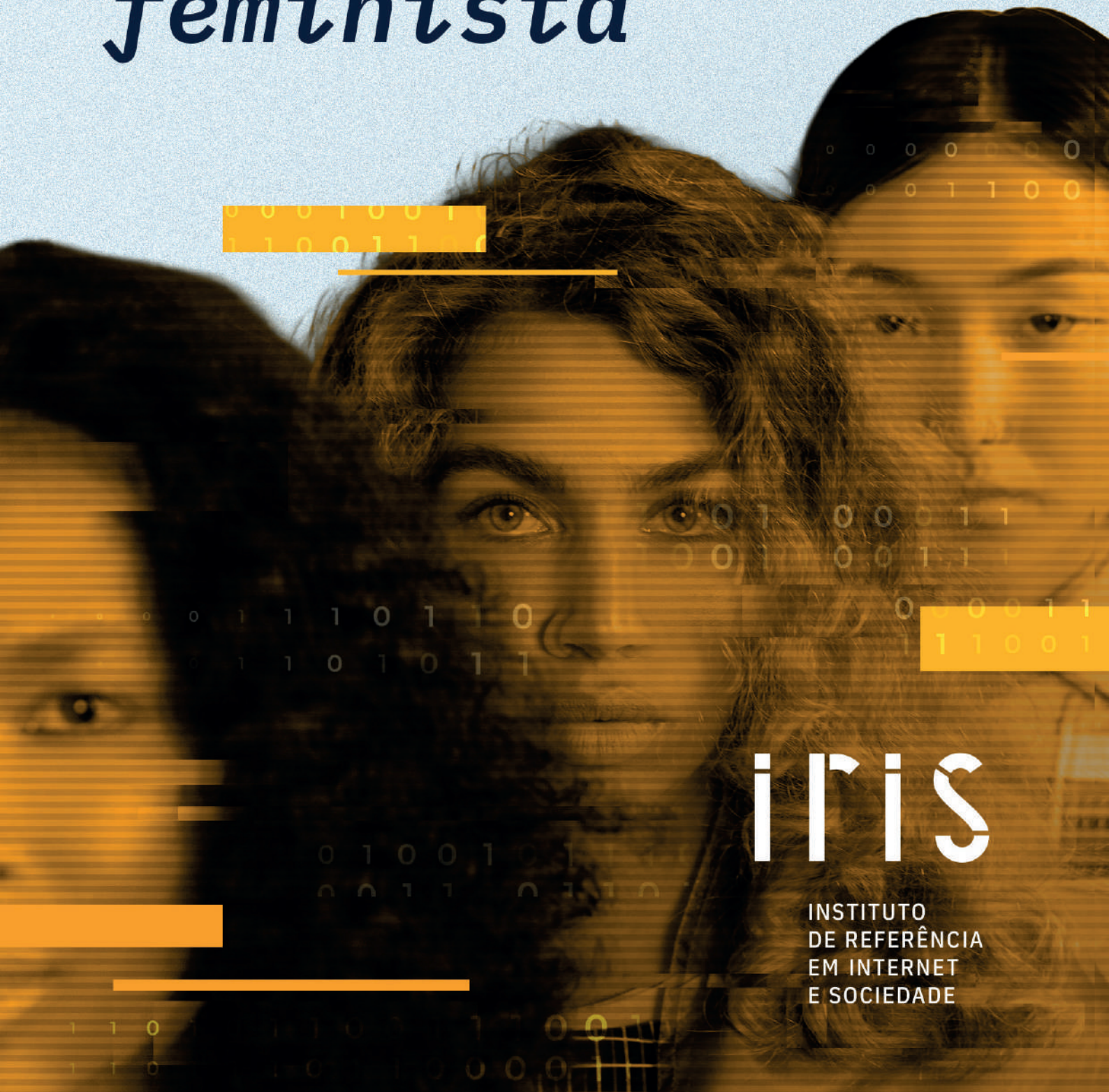
Policy Brief

Criptografia como uma questão *feminista*



INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE

Agradecemos à equipe da Chayn por autorizar a tradução deste material, tornando suas pesquisas sobre criptografia e segurança feminista acessíveis em português. Para referência, seguem os links originais:

Versão em inglês do blog:
https://c.chayn.co/3OPdtN4

Relatório completo sobre Criptografia:
https://c.chayn.co/4u2zusf

Site da Chayn:
https://c.chayn.co/4aIeNJ8

Policy Brief

Criptografia como uma questão feminista

Por que formuladores de políticas públicas e organizações da sociedade civil devem compreender o papel que a criptografia desempenha na proteção das comunidades que apoiam.

Este documento foi elaborado para subsidiar formuladores de políticas públicas e suas equipes técnicas que lidam com a regulação da criptografia, das tecnologias de comunicação e da cibersegurança. O objetivo é contextualizar a importância criptografia como uma pauta feminista, analisando seu impacto sobre a privacidade e a segurança de mulheres e de pessoas de gêneros dissidentes em diferentes contextos ao redor do mundo.

O material também é voltado a gestores e organizações da sociedade civil que trabalham no enfrentamento da violência de gênero, destacando o papel fundamental da criptografia na proteção das comunidades com as quais trabalham.

O que é criptografia de ponta a ponta?

A criptografia é o processo de codificação de dados que garante que a informação só seja acessível aos seus legítimos destinatários. Ela protege diferentes esferas da nossa vida digital, abrangendo desde a troca de e-mails e mensagens privadas até a segurança das informações sensíveis que guardamos em nossos dispositivos. No entanto, o nível de proteção oferecido não é uniforme em todas as aplicações. É relativamente comum que provedores de serviço retenham a capacidade de acessar o conteúdo das comunicações, o que gera riscos e vulnerabilidades à privacidade.

É justamente nesse cenário que a criptografia de ponta a ponta se diferencia ao impedir qualquer tipo de acesso intermediário. Através dela, apenas quem envia e quem recebe uma mensagem pode acessar seu conteúdo. Uma forma didática de compreendê-la é imaginá-la como uma carta protegida por um cadeado, cuja chave pertence exclusivamente ao remetente e ao destinatário. Nenhum terceiro - nem mesmo a empresa que fornece o serviço - pode acessar a mensagem.

Por esse motivo, a criptografia de ponta a ponta é amplamente reconhecida como uma tecnologia essencial para a proteção da privacidade e da segurança. Ela é adotada e recomendada por prestadores de serviços financeiros, por governos (como boa prática prevista no Regulamento Geral de Proteção de Dados do Reino Unido - UK GDPR), por organizações internacionais, incluindo as Nações Unidas, e por plataformas de comunicação online. Serviços populares como WhatsApp, Signal e Facebook Messenger utilizam criptografia de ponta a ponta para proteger mensagens e chamadas, inclusive em comunicações em grupo.

Por que a criptografia é uma questão feminista?

A criptografia desempenha um papel fundamental na proteção dos direitos e da segurança de mulheres e de pessoas de gêneros dissidentes em diferentes contextos. Nesta seção, exploramos três situações centrais em que a criptografia atua como uma ferramenta crítica de proteção: no apoio a sobreviventes de violência doméstica, na garantia de acesso seguro a serviços de aborto e no fortalecimento do ativismo feminista.

Apoio a sobreviventes de violência doméstica

A perda de privacidade é um elemento central e profundamente destrutivo da violência doméstica. Quando uma pessoa vive com seu agressor, nem mesmo o próprio lar pode ser considerado um espaço seguro. Para muitas sobreviventes, a violência não se encerra com a saída de casa: práticas contínuas de perseguição e assédio por ex-parceiros frequentemente prolongam o ciclo de abuso, comprometendo sua autonomia e violando seu direito ao espaço pessoal.

Nesse cenário, a existência de canais seguros de comunicação entre sobreviventes e abrigos ou organizações de apoio não é apenas uma medida de

proteção, mas um passo fundamental para a reconstrução do exercício do direito humano à privacidade, à autonomia e à segurança.

No âmbito de suas pesquisas, a Chayn observou que, especialmente no continente africano, tornou-se cada vez mais comum que abrigos e organizações de apoio permitam que sobreviventes estabeleçam contato por meio de canais digitais. Entre os exemplos estão o National Shelter Movement, na África do Sul; a Women Safe House, na Nigéria; a AlertGBV, em Camarões; e o uso do WhatsApp como ferramenta de comunicação. Em Moçambique, durante os períodos de confinamento impostos pela pandemia de COVID-19, organizações que atuam no enfrentamento da violência de gênero passaram a utilizar o WhatsApp para prover atendimento a mulheres que vivenciaram abusos domésticos.

Além disso, a criptografia é particularmente essencial em contextos em que o parceiro agressor dispõe de conhecimentos técnicos ou recursos financeiros capazes de viabilizar a interceptação de comunicações. O risco de vigilância e controle é ainda mais elevado quando a vítima de violência doméstica manteve relações com homens empregados em forças de segurança pública ou em empresas de telecomunicações. Nessas situações, o agressor pode ter acesso privilegiado a ferramentas, conhecimentos ou redes que permitem formas mais sofisticadas de monitoramento e coerção. Esse dado é especialmente relevante à luz de pesquisas que documentam a incidência de violência doméstica entre profissionais das forças de segurança, como demonstrado, por exemplo, no Reino Unido.

Proteção no acesso à saúde reprodutiva

Com o aumento das restrições legais ao aborto em alguns países, incluindo os Estados Unidos, abrigos que oferecem acesso a esse procedimento passaram a recorrer à criptografia tanto para garantir um aborto seguro, quanto para proteger mulheres que buscam este procedimento, perante órgãos de segurança e grupos anti aborto.

Em entrevista à NBC, Gabrielle Goodrick, proprietária da Camelback Family Planning, em Phoenix, afirmou que a incerteza sobre possíveis consequências levou sua equipe a substituir formas de comunicação que deixavam "pegadas digitais", por chamadas telefônicas e aplicativos de mensagens criptografadas.

O serviço de aborto Hey Jane, que fornece pílulas abortivas, também disponibiliza um guia de privacidade digital, com opções de comunicação criptografada para quem busca o aborto.

Grupos que defendem o aborto ou oferecem suporte legal a pessoas que realizaram o procedimento também dependem da criptografia. A rede de advogados pela justiça reprodutiva If/When/How oferece dicas de segurança digital e, em entrevista ao *Politico*, explicou que sua linha direta permite que as pessoas enviem perguntas por plataformas seguras, como Signal e Proton Mail.

A criptografia é igualmente importante para organizar protestos sobre temas sensíveis. Por exemplo, o grupo ativista Abortion Access Front utiliza o Signal durante suas manifestações.

Sobre o plano da Meta de implementar criptografia de ponta a ponta no Messenger, Shireen Rose Shakouri, vice-diretora da Reproaction - grupo de ação direta que busca ampliar o acesso ao aborto e promover justiça reprodutiva, afirmou:

> *"A privacidade online é essencial para quem busca o aborto, e comunicações seguras devem ser prioridade para empresas de tecnologia que querem proteger informações de saúde pessoal contra invasões, criminalização e estigmatização. A Reproaction apoia qualquer esforço para aprimorar a criptografia de ponta a ponta e continuará acompanhando o progresso nesse objetivo tão necessário."*

A necessidade de comunicações seguras nesses casos não se limita aos EUA. No México, o bloqueio da conta de WhatsApp de um provedor de abortos deixou mulheres que buscam aborto sem respostas e sem suporte essencial. A MSI Foundation (antiga Marie Stopes) relatou queda de 80% nos atendimentos no dia seguinte ao bloqueio. Embora não esteja claro o motivo do bloqueio da conta, alguns atribuem o caso à aplicação excessiva das políticas da Meta por meio de inteligência artificial, enquanto outros veem como resultado de uma campanha organizada por grupos antiaborto. Esse episódio evidencia a necessidade urgente de criptografia para que as mulheres possam acessar o aborto de forma segura.

Potencializando o ativismo feminista

Como mostram os casos de grupos de apoio ao aborto, a criptografia pode ser um instrumento decisivo para o ativismo feminista. Em alguns países, ela separa a expressão da censura, e a liberdade da prisão - sendo por vezes uma questão de vida ou morte.

Um relatório de 2023 da Human Rights Watch identificou que forças de segurança no Egito, Iraque, Jordânia, Líbano e Tunísia perseguiam membros de comunidades queer com base em suas atividades em redes sociais e aplicativos de encontros, levando a processos criminais, tortura e outros abusos fora do ambiente digital. De forma preocupante, o relatório também apontou que cidadãos "comuns", e não apenas autoridades, contribuíam para essa perseguição.

Depois da Revolução Verde de 2009, o parlamento iraniano proibiu o uso de criptografia. Mesmo assim, os iranianos continuaram a usar aplicativos estrangeiros criptografados, como o WhatsApp. De acordo com Mahsa Alimardani, pesquisadora da Universidade de Oxford e especialista em liberdade de expressão online no Artigo 19, esses aplicativos tiveram um papel essencial na organização de protestos.

Diante da ameaça de regimes opressores, outras comunidades em situação de risco também passaram a recorrer a plataformas criptografadas para se proteger. Após a tomada do Afeganistão pelo Talibã em 2021, a ONG americana Operation Recovery utilizou o AWS Wickr, um serviço com criptografia de ponta a ponta, para evacuar milhares de afegãos do país, incluindo ativistas e jornalistas que corriam risco de serem executados.

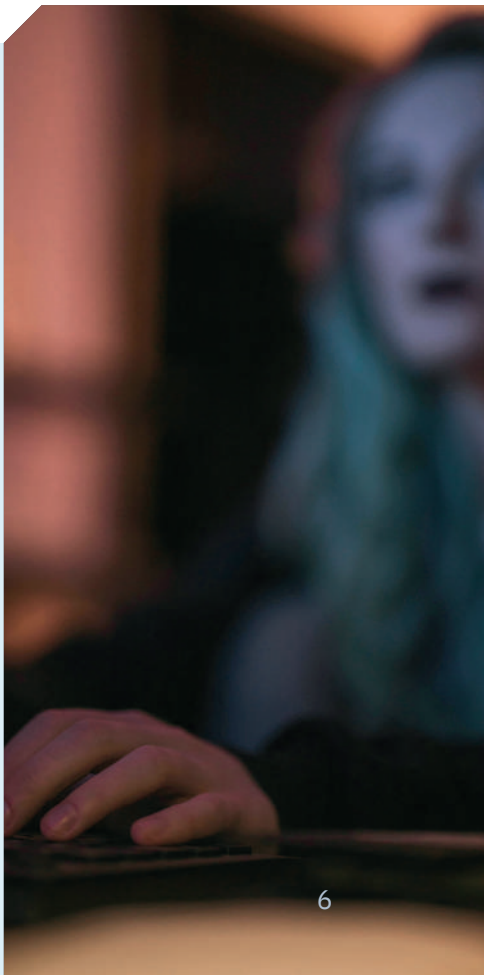
Ainda no Afeganistão, a Meta registrou que uma equipe feminina de futebol usava o WhatsApp para se reunir e conversar, com medo de que o Talibã as perseguisse ou tentasse interceptar suas comunicações.

Esses exemplos mostram claramente que a criptografia não é um luxo — é uma questão de sobrevivência. Para ativistas feministas, sobreviventes de violência de gênero e comunidades marginalizadas em todo o mundo, a comunicação segura é essencial para conseguir apoio e participar de ações de ativismo. Garantir a proteção da criptografia forte globalmente, portanto, não é apenas uma questão técnica; é uma questão de direitos humanos. À medida que as ameaças à privacidade e à segurança digital aumentam ao redor do mundo, manter o acesso à criptografia de ponta a ponta deve ser uma prioridade para todos que defendem justiça, igualdade e a proteção das pessoas mais vulnerabilizadas.

O que precisa ser feito a seguir

Como este briefing demonstrou, a criptografia é uma questão feminista, e sua proteção é essencial para garantir os direitos, a segurança e a dignidade de mulheres e pessoas de minorias de gênero em todo o mundo. Para atender a essa necessidade, as empresas devem priorizar a implementação da criptografia de ponta a ponta em suas plataformas, por padrão e sem exceções, Esse recurso não deve ser um privilégio ou uma exceção, mas a regra para qualquer comunicação digital segura.

Ao mesmo tempo, os governos têm a responsabilidade de apoiar e proteger a criptografia forte, resistindo a tentativas de enfraquecê-la por leis ou backdoors. Garantir comunicações seguras e privadas não se trata apenas de segurança digital - é também uma questão de direitos humanos e justiça de gênero.



iris

INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE