Contribuição à Chamada Pública:

"**Fighting Child Sexual Abuses:** detection, removal and reporting of illegal content online"

da Comissão Europeia

IP.rec
INSTITUTO DE PESQUISA EM DIREITO & TECNOLOGIA DO RECIFE

INSTITUTO DE PESQUISA EM
DIREITO & TECNOLOGIA DO RECIFE

Nosso **trabalho** e **contexto**

O Instituto de Pesquisa em Direito e Tecnologia do Recife - IP.rec é um centro independente de pesquisa e incidência política brasileiro com foco na análise de políticas públicas e fenômenos tecnológicos que afetem o ecossistema de direitos na Internet.

O IP.rec tem atuação de referência nas áreas de privacidade, segurança e tecnologias de vigilância, com ênfase em políticas de criptografia, tendo publicado estudos ao longo de sua atuação, entre eles o "Mosaico Legislativo da Criptografia no Brasil: uma análise de Projetos de Lei", e a Cartilha "A Importância Social e Econômica da Criptografia",[1] além da organização de vários eventos de caráter multissetorial tendo como objeto a criptografia. A organização integra a Coalizão Direitos na Rede e a Global Encryption Coalition, redes de entidades da sociedade civil e da comunidade técnica e científica cuja missão tem foco na proteção dos direitos digitais e, em especial, da criptografia.

De antemão, portanto, cumpre destacar que o combate ao abuso sexual infantil online e suas formas de distribuição devem ser encarados como prioridade nas agendas políticas nacionais. Entende-se que o enfrentamento do problema deve se dar de forma global e mediante cooperação entre os diversos atores responsáveis, sejam agências de investigação locais, federais e internacionais, bem como provedores de aplicação e entidades da sociedade civil de interesse especial. As áreas de combate ao abuso sexual infantil, portanto, deve observar estritamente as necessidades de segurança e garantia de direitos na Internet, como forma de criar um ambiente confiável e resiliente para o público infantil. O IP.rec, portanto, saúda a iniciativa de tomada de subsídios por parte da Comissão Europeia.

[1] Em parceria com o Instituto de Referência em Internet e Sociedade (IRIS)

Criptografia, segurança e sociedade

O IP.rec compreende que enquanto estratégias de combate ao abuso sexual infantil estão sendo traçadas no âmbito da União Europeia, tecnologias que atualmente são estabelecidas como meio de proteção às comunicações estão sendo endereçadas como pontos de atenção. Documentação desenvolvida no âmbito da Comissão Europeia e vazada em setembro de 2020, por exemplo, sugere que a criptografia deve ser um "desafio" a ser enfrentado no contexto da agenda da presente chamada. Essa compreensão, portanto, é nociva a uma visão complexa e integral da governança multissetorial da Internet, em que direitos e interesses dos variados agentes estatais, tecnológicos e socioeconômicos dependem de redes com criptografia forte.

A expansão do uso da Internet e de dispositivos conectados não leva em consideração a idade dos indivíduos e abarca os mais diversos públicos, sejam eles adultos, idosos, crianças ou adolescentes. A infraestrutura e os protocolos dos quais a segurança da Internet depende, portanto, devem ser encarados de forma holística, não-etária e deve abranger a totalidade e diversidade de usos da rede. Isso quer dizer que transações bancárias, envio de e-mails, atividades industriais, mensagens privadas, trabalhos de investigação jornalística, comunicações políticas sensíveis e mesmo a segurança de jogos online ou brinquedos conectados dependem de padrões mínimos de segurança. Sua vulnerabilização, ainda que discreta, pode comprometer indivíduos física, econômica e psicologicamente. A proteção de um ponto da rede é suficientemente significativa para todo o ecossistema. Da mesma forma, a vulnerabilização de um único ponto pode gerar efeitos estruturais e sistêmicos para a cadeia de conectividade da Internet.

Enquanto elemento chave da segurança da informação desses sistemas, a criptografia acompanhou o desenvolvimento comercial da Internet e está historicamente presente no tráfego de informações e no armazenamento de dados pessoais. Gera resiliência e confiabilidade à rede ao proteger a confidencialidade de informações, autenticidade das identidades envolvidas em uma troca de mensagens - sejam entre pessoas, pessoas e máquinas e entre várias máquinas - e integridade ao fluxo de dados, sem as quais o uso de dispositivos conectados (de smartphones acarros ou objetos domésticos) geraria mais riscos à sociedade do que novas potencialidades.

Do ponto de vista legal e político, o uso de aplicações que agregam múltiplas tecnologias e protocolos criptográficos é basilar para o exercício de direitos. Testemunhas e vítimas podem se comunicar com autoridade sem receio ou inibição, investigações podem ser conduzidas sem que haja interferência ou sabotagem, jornalistas podem assegurar o sigilo de suas fontes, assim como dissidentes e minorias em regiões de crise política podem denunciar abusos e violação de direitos sem que sejam perseguidos por isso.

É consolidado, portanto, que a criptografia é ferramenta instrumental ao exercício integral de direitos humanos e políticos e central para a autodeterminação informacional dos indivíduos.

Proteção da criança no ecossistema da Internet

Para a Convenção sobre o Direito das Crianças das Nações Unidas, crianças e adolescentes são sujeitos de direitos e destinatários prioritários das políticas de bem-estar social e psicológico. A Convenção estabelece que crianças possuem liberdade para se expressar livremente, tanto na procura e na recepção quanto na divulgação de informações e ideias de todos os tipos. Da mesma forma, é protegido o direito das crianças em acessar informações e materiais procedentes de diversas fontes, sejam elas nacionais ou internacionais. Como forma de potencializar o acesso à informação - elemento fundamental na formação da personalidade de crianças e adolescentes - o estabelecimento de redes seguras e confiáveis deve ser priorizado.

A UNICEF estipula que, entre as formas essenciais para se alcançar o bem-estar das crianças e adolescentes na Internet, está a garantia de que indústrias de tecnologia, principalmente as redes sociais, garantam uma plataforma online que proporcione a sua proteção. É conclusivo, portanto, que crianças e adolescentes, enquanto público alvo cuja proteção deve ser ainda mais reforçada, são elos onde a criptografia deve atuar de forma ainda mais robusta, reduzindo as margens para ataques maliciosos (seja a dados armazenados ou em trânsito, no uso de dispositivos por crianças e adolescentes) acessos não autorizados e outras ameaças em franca expansão no ambiente online.

A racionalidade de permitir brechas que facilitem o alcance de representações investigativas/policiais sobre comunicações - das quais crianças fazem parte direta ou indiretamente - amplia o risco de legitimar, ainda mais, a ampliação das formas de monitoramento e filtragem de conteúdos. Atualmente, uma diversidade de dispositivos e aplicações orbitam o ambiente da criança, como babás eletrônicas, brinquedos conectados e mesmo celulares, tablets e laptops. Afastar a autonomia informacional das crianças e de seus responsáveis sobre a acessibilidade e sigilo dessas informações tem o condão de violar a privacidade desse público e de círculos de convivência profundamente íntimos.

Esse cenário é ainda mais agravado em tempos de pandemia e isolamento social, em que os níveis de tempo de conexão à Internet alcançam níveis inéditos. A quase totalidade das atividades educacionais e interações sociais migram para a Internet, situação que reforça o estabelecimento de protocolos

e compromissos de segurança tanto por parte das plataformas e agentes governamentais quanto pelos núcleos familiares, sociais e educacionais. Os danos resultantes de ventuais inserções de vulnerabilidades e tecnologias de monitoramento nesses sistemas poderão gerar danos irreparáveis à integridade e formação psicológica de crianças e adolescentes.

A experiência brasileira com políticas de criptografia

Entre 2015 e 2016, o aplicativo de mensagens WhatsApp foi efetivamente bloqueado por três vezes no Brasil em razão de ordens judiciais no âmbito de investigações criminais (em todas elas com posterior reversão das decisões por tribunais de instâncias superiores). Os fatos repercutiram publicamente no país e no mundo em razão dos prejuízos políticos e sociais, bem como à cadeia econômica e tecnológica doméstica e extraterritorial dependente da criptografia. Catalisaram, portanto, inúmeros debates, pesquisas, campanhas e precedentes judiciais de relevância global.

Como consequência, duas ações tramitam perante o Supremo Tribunal Federal (STF) e ambas têm por objeto a pretensa possibilidade de que sejam bloqueadas aplicações em razão do uso de criptografia ponta-a-ponta.2 Ainda que os processos estejam em andamento, os votos dos juízes relatores das duas ações são paradigmáticos quanto ao entendimento constitucional no Brasil sobre a legalidade e central importância do uso de criptografia forte no país. Para a Ministra Rosa Weber, do STF, seriam inconstitucionais medidas governamentais que obrigassem agentes privados a inserir em seus sistemas recursos adicionais que possibilitem o acesso a quaisquer elementos do conteúdo das conversas, ou mesmo formas de responsabilizá-los em caso de descumprimento: “não pode o Estado compeli-lo [o agente privado] a oferecer um serviço menos seguro e vulnerável”.

A Ministra do STF Rosa Weber igualmente desloca o debate para longe da falsa dicotomia entre “privacidade e segurança”, uma vez que “a mesma tecnologia que tornaria mais fácil às autoridades de segurança pública acessarem conteúdo armazenado pode – e, existindo, será – utilizada por criminosos para terem acesso a informações privadas de futuras vítimas”. A lógica se aplica com ainda mais ênfase no contexto da proteção à criança e ao adolescente, cujas informações são mais sensíveis.

---

[2] Em 2017, Audiência Pública foi convocada pelo Supremo Tribunal Federal no âmbito dos dois processos. Cerca de trinta organizações e entidades vinculadas ao setor público, privado, comunidade científica e tecnológica, bem como organizações da sociedade civil foram ouvidas para a formação de entendimento dos juízes da Corte.

Sua proteção, caso insuficiente, pode gerar novas brechas de segurança que ensejariam na exploração por aqueles envolvidos em redes de disseminação de conteúdo sexual infantil. Consequentemente, uma eventual estratégia de combate levaria a multiplicação de casos.

A demanda por criptografia nas comunicações, portanto, é derivada da legítima expectativa do usuário, em um contexto social democrático, de que não seja afetada sua liberdade de expressão por nenhuma interferência tecnológica. Isso é o que reafirma o Ministro do STF Edson Fachin, acrescentando que é do nteresse dos agentes estatais que não sejam criadas exceções, mas que seja encorajada a implementação de recursos de criptografia por parte do setor empresarial tendo em vista tanto o exercício de direitos políticos quanto a resiliência dos recursos de segurança da rede. Esse entendimento se alia, inclusive, à compreensão da Comissão de Direitos Humanos da ONU, a qual vêm marcadamente desencorajando qualquer espécie de interferência na criptografia por parte dos Estados.

O entendimento do STF, até então, sinaliza para uma necessária conciliação dos agentes de segurança pública com as plataformas de criptografia. Ainda que seja prioritária e urgente a criação de frentes de combate ao abuso sexual infantil, inclusive com o auxílio de novas tecnologias, não há de se perder de vista a macro-estrutura de direitos e infraestruturas de segurança dependentes de robustos padrões criptográficos. Além disso, o problema em questão é suficientemente complexo para ser visto apenas pela variável tecnológica: considerada unicamente apenas essa perspectiva, perde-se de vista o problema que se busca resolver e o expõe a novas superfícies de ataque.

Testes necessários: eficácia, necessidade e proporcionalidade

Não são poucas as supostas soluções sugeridas por agências de inteligência e investigação como forma de alcançar o inalcançável: criar exceções de acesso, sistemas de custódia de chaves-mestras, filtragem de conteúdo, rastreamento de mensagens, “usuários fantasmas”, entre outros - “sem que seja afetada a criptografia” (sic).

Ainda que legítimas e relevantes as causas de onde partem as propostas (combate a crimes hediondos, incluindo o abuso sexual infantil), é difícil encontrar medidas de natureza tecnológica, no campo da criptografia, que não avancem sobre outros direitos dos indivíduos e/ou que sejam pouco eficazes.

Portanto, testes de eficácia, necessidade e proporcionalidade devem preceder qualquer construção de política pública que busque endereçar formas de combate ao abuso sexual infantil online. Do contrário, estaríamos diante do regresso de décadas de desenvolvimento de técnicas de autenticação, sigilo e integridade de comunicações; de um aumento nocivo da complexidade na arquitetura da segurança em aplicações; e da criação de novos focos de ataque que irão explorar as vulnerabilidades criadas.

Em termos de alcance de resultados, a inserção de novos recursos em aplicações de mensageria (como client-side scanning, comumente exemplificado pelo PhotoDNA) deve levar em consideração que é relativamente simples e intuitivo que atores maliciosos apenas migrem para outras plataformas, o que tornaria rapidamente ineficaz a medida. Isso levaria a uma incansável distribuição mandatória de ferramentas de filtragem de conteúdo - em um contexto em que novas aplicações são postas à disposição todos os dias - o que oneraria os esforços das forças de investigação e, ao mesmo tempo, não alcançaria uma escalabilidade eficaz.

Imprescindível, igualmente, seria pensar para além da mera "utilidade" da medida e comprovar que a eventual solução adotada seria a menos intrusiva à privacidade dos usuários e a que causaria menor impacto à segurança da rede. Ou seja, seria necessário apontar, por meio de dados suficientes e relevantes, bem como instrumentos de avaliação de impacto aos direitos e ao ecossistema da Internet (com a colaboração de especialistas de variadas disciplinas), que a medida é necessária para alcançar a finalidade específica pretendida. Até então, não são identificadas, no âmbito das articulações da Comissão Europeia, publicações que acolham suficientemente o tema e se mostrem capazes de orientar avaliações de impacto dessas medidas dessa natureza tão intrusiva.

Ao mesmo tempo, a título de combater crimes específicos, busca-se criar um mecanismo que poderá afetar, desproporcionalmente, bilhões de usuários de aplicativos de mensagem, redes sociais e da uma multiplicidade de redes e serviços que funcionam por meios interoperáveis. Do ponto de vista da finalidade, não tardaria para que um eventual recurso de filtragem de imagens seja utilizado para outras mídias, como textos e voz e vídeos cujo conteúdo não tenha relação com o combate ao abuso sexual infantil. A ampliação inesgotável de um "biblioteca da censura" via filtragem de conteúdo é exemplificada pelo WeChat, na China, como apontado pelo Citizen Lab.

No fim do dia, soluções de client-side scanning, por exemplo, não seriam diferentes de filtragem diretamente via servidor do provedor, o que significaria um comprometimento da criptografia por outros meios.

Portanto, testes de eficácia, necessidade e proporcionalidade devem preceder qualquer construção de política pública que busque endereçar formas de combate ao abuso sexual infantil online. Do contrário, estaríamos diante do regresso de décadas de desenvolvimento de técnicas de autenticação, sigilo e integridade de comunicações; de um aumento nocivo da complexidade na arquitetura da segurança em aplicações; e da criação de novos focos de ataque que irão explorar as vulnerabilidades criadas.

Em termos de alcance de resultados, a inserção de novos recursos em aplicações de mensageria (como client-side scanning, comumente exemplificado pelo PhotoDNA) deve levar em consideração que é relativamente simples e intuitivo que atores maliciosos apenas migrem para outras plataformas, o que tornaria rapidamente ineficaz a medida. Isso levaria a uma incansável distribuição mandatória de ferramentas de filtragem de conteúdo - em um contexto em que novas aplicações são postas à disposição todos os dias - o que oneraria os esforços das forças de investigação e, ao mesmo tempo, não alcançaria uma escalabilidade eficaz.

Imprescindível, igualmente, seria pensar para além da mera "utilidade" da medida e comprovar que a eventual solução adotada seria a menos intrusiva à privacidade dos usuários e a que causaria menor impacto à segurança da rede. Ou seja, seria necessário apontar, por meio de dados suficientes e relevantes, bem como instrumentos de avaliação de impacto aos direitos e ao ecossistema da Internet (com a colaboração de especialistas de variadas disciplinas), que a medida é necessária para alcançar a finalidade específica pretendida. Até então, não são identificadas, no âmbito das articulações da Comissão Europeia, publicações que acolham suficientemente o tema e se mostrem capazes de orientar avaliações de impacto dessas medidas dessa natureza tão intrusiva.

Ao mesmo tempo, a título de combater crimes específicos, busca-se criar um mecanismo que poderá afetar, desproporcionalmente, bilhões de usuários de aplicativos de mensagem, redes sociais e da uma multiplicidade de redes e serviços que funcionam por meios interoperáveis. Do ponto de vista da finalidade, não tardaria para que um eventual recurso de filtragem de imagens seja utilizado para outras mídias, como textos e voz e vídeos cujo conteúdo não tenha relação com o combate ao abuso sexual infantil. A ampliação inesgotável de um "biblioteca da censura" via filtragem de conteúdo é exemplificada pelo WeChat, na China, como apontado pelo Citizen Lab.

No fim do dia, soluções de client-side scanning, por exemplo, não seriam diferentes de filtragem diretamente via servidor do provedor, o que significaria um comprometimento da criptografia por outros meios.

Conclusão

O IP.rec elogia, uma vez mais, a chamada de contribuições e reforça a necessidade de debates e processos consultivos de natureza multissetorial. Entende, também, que o tema é de interesse público e transcende fronteiras nacionais.

Logo, a tomada de subsídios deve ser ampla e levar em consideração a experiência de outros territórios, tendo em vista o caráter transfronteiriço da Internet e os efeitos indesejados que políticas públicas podem causar à integridade dos sistemas tecnológicos globais. Ressaltamos, por fim, os pontos acima destacados para reafirmar que eventuais soluções adotadas no contexto do combate ao abuso sexual infantil não devem subestimar efeitos colaterais que possam ser gerados ao direitos individuais e coletivos dos usuários, uma vez que o exercício da cidadania e da democracia se relaciona, cada vez mais, com um complexo ambiente digital.


IP.rec
INSTITUTO DE PESQUISA EM
DIREITO & TECNOLOGIA DO RECIFE