Internet Society
Capítulo Brasil

Manifestação sobre a decisão da ANPD que determinou a suspensão da funcionalidade "Go Live" no Discord

A ISOC Brasil acompanha com atenção e apoia a medida preventiva adotada pela Agência Nacional de Proteção de Dados (ANPD) em face do Discord. A Agência determinou a suspensão, no território nacional, da funcionalidade "Go Live" e de recursos equivalentes de transmissão e compartilhamento de vídeo até que a plataforma demonstre a adoção de medidas adequadas aos riscos identificados para crianças e adolescentes.

A gravidade dos fatos que motivaram a atuação da ANPD exige resposta efetiva. Plataformas digitais que operam no Brasil devem cumprir a legislação brasileira e adotar medidas proporcionais para prevenir, identificar, interromper e mitigar riscos associados às funcionalidades que oferecem. Elas não podem invocar a utilização de criptografia de ponta a ponta (E2EE) , por si só, como fundamento para afastar suas obrigações legais.

Ao mesmo tempo, o cumprimento da legislação não deve ser entendido como uma exigência de que o provedor tenha acesso ao conteúdo das comunicações. A proteção de crianças e adolescentes e a preservação de comunicações seguras não constituem objetivos concorrentes.

Como a ISOC Brasil tem defendido em suas contribuições sobre a implementação do ECA Digital, as responsabilidades de cada agente devem ser definidas de maneira proporcional aos riscos envolvidos, às funções desempenhadas e às capacidades de intervenção que efetivamente decorrem dos recursos sob seu controle. Nessa linha, obrigações legítimas de proteção não devem ser convertidas em exigências de enfraquecimento da criptografia.

É justamente sob essa perspectiva que alguns trechos da Nota Técnica nº 1/2026/CGF/SFI/ANPD merecem maior precisão. O documento reconhece corretamente que, em uma arquitetura de criptografia de ponta a ponta, o provedor não tem acesso ordinário ao conteúdo das comunicações enquanto elas ocorrem, pois o áudio e o vídeo são cifrados no dispositivo de quem envia e decifrados no dispositivo de participantes que recebem.

Em determinadas passagens, entretanto, a linguagem adotada pela Nota Técnica da ANPD, se interpretada de forma que a ISOC Brasil considera inadequada, pode produzir uma associação excessivamente abrangente entre a implementação da criptografia e uma suposta incapacidade da plataforma de cumprir seus deveres de proteção. Em especial, há esse risco de má interpretação onde a Nota relaciona a baixa observabilidade das normas legais por determinados ambientes digitais à "implementação proativa de criptografia"; e na afirmação genérica de que "a criptografia impede o acesso direto da plataforma ao conteúdo durante a interação".

Embora seja tecnicamente correto afirmar que a E2EE restringe uma capacidade específica do provedor, qual seja, acessar ordinariamente o conteúdo em claro e realizar sobre ele determinadas modalidades de inspeção centralizada, dessa limitação não decorre que desapareçam os demais recursos técnicos, informacionais e organizacionais disponíveis ao serviço, tampouco as capacidades de prevenção, mitigação e resposta que podem ser construídas a partir deles. A criptografia pode, portanto, modificar os meios pelos quais determinada obrigação é cumprida, mas não constitui, em si mesma, impedimento ao seu cumprimento.

Ao examinar comunicações protegidas por E2EE, a ANPD reconhece que a ausência de acesso direto ao conteúdo não elimina as possibilidades de atuação da plataforma, que pode recorrer a controles no dispositivo, sinais comportamentais, restrições de produto, mecanismos de denúncia e outras salvaguardas.

Embora a E2EE retire do provedor a capacidade ordinária de acessar o conteúdo das comunicações, outras capacidades de proteção permanecem disponíveis, como controles sobre funcionalidades, aferição etária, sinais comportamentais, mecanismos de denúncia e protocolos de interrupção. Obrigar um provedor a criar capacidade permanente de acesso ao conteúdo, por outro lado, altera a arquitetura de segurança do sistema e introduz novos riscos.

Assim, a ISOC Brasil tem defendido que dificuldades de investigação, moderação ou fiscalização não justificam portas clandestinas (*backdoors*), acesso excepcional ou outras formas de enfraquecimento da criptografia[1]. A análise regulatória deve se concentrar na suficiência dessas outras medidas, sem tomar o acesso ao conteúdo como parâmetro geral de conformidade.

Ao mesmo tempo, existem alternativas compatíveis com E2EE, como cautela também é necessária quanto à referência da Nota Técnica à “detecção no dispositivo”, expressão que pode abranger soluções muito distintas. Processamento local voltado à proteção do próprio usuário não se confunde com *client-side scanning*, que introduz mecanismos sistemáticos de inspeção das comunicações e pode ampliar superfícies de ataque e riscos de uso indevido. Por isso, a referência da ANPD não deve ser interpretada como autorização genérica para varredura de comunicações, assim como a exigência de “efetividade equivalente ou superior” deve se referir à mitigação do risco, e não à reprodução do mesmo grau de acesso ao conteúdo existente em sistemas sem E2EE.

A exigência de “mecanismos tecnicamente eficazes contra burla” também deve ser interpretada de forma restrita à evasão da medida por recursos sob controle efetivo da

[1] Ver: Solving Crime Without Breaking Encryption. Disponível em: https://www.internetsociety.org/blog/2026/06/solving-crime-without-breaking-encryption/

plataforma, não devendo servir de fundamento, sem previsão expressa e análise de proporcionalidade, para restrições generalizadas a tecnologias de uso legítimo, como VPNs.

Também importa ressaltar que a preocupação central orbita a proteção integral de crianças e adolescentes, objeto de prioridade absoluta garantida constitucionalmente e regulada pelo ECA Digital. As demandas desse tema, todavia, não devem ser indistintamente estendidas para contextos de comunicação entre pessoas adultas. Por isso mesmo, é crucial avançar na adoção de medidas adequadas e mecanismos para mitigar riscos identificados para crianças e adolescentes.

A ISOC Brasil entende, portanto, que a medida adotada pela ANPD deve ser implementada de forma proporcional, baseada em risco e compatível com a arquitetura do serviço, considerando os recursos sob controle do provedor e as capacidades de proteção que deles decorrem. Para as próximas etapas de fiscalização e regulamentação do ECA Digital, recomenda-se que a ANPD preserve essa distinção, reconhecendo que a criptografia não pode servir de justificativa para a ausência de salvaguardas adequadas, mas tampouco deve ser tratada, por si só, como evidência de descumprimento ou como obstáculo à proteção de crianças e adolescentes. A atuação regulatória deve, assim, incentivar soluções efetivas de prevenção e resposta que preservem a confidencialidade, a integridade e a segurança das comunicações dos usuários.