

Responsabilidade dos provedores de internet no combate à exploração sexual infantil

27/10/2024

Nos Estados Unidos, empresas digitais são legalmente obrigadas a relatar qualquer conteúdo relacionado à exploração sexual infantil, incluindo pedofilia, ao Centro Nacional para Crianças Desaparecidas e Exploradas (*National Center for Missing and Exploited Children* — NCMEC). Essa obrigação abrange qualquer material envolvendo abuso sexual infantil, seja ele detectado em mensagens, fotos ou qualquer outro tipo de mídia, mesmo que compartilhado em plataformas privadas.

Essa exigência deriva do *CyberTipline Reporting Obligation*, estabelecido no Title 18, United States Code, Seção 2258A. A lei determina que provedores de serviços de internet e tecnologia (como ISPs, plataformas de mídia social e serviços de e-mail) que tomem conhecimento de abuso ou pornografia infantil em suas plataformas devem relatar o caso imediatamente ao NCMEC.

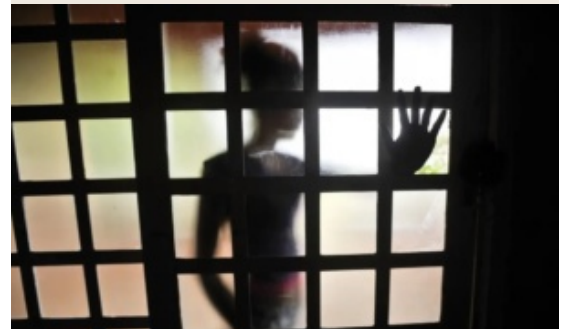
Embora a legislação não obrigue as empresas a monitorarem proativamente as comunicações, elas devem relatar qualquer conteúdo de abuso sexual infantil que detectarem, seja por meio de denúncias de usuários ou através de algoritmos internos de moderação. Isso inclui o uso de sistemas automatizados para identificar imagens conhecidas de abuso sexual infantil (como o *hash matching*).

Além disso, o NCMEC colabora com autoridades policiais, que investigam os casos e tomam medidas para identificar suspeitos, proteger as vítimas e combater crimes dessa natureza. Essas investigações são realizadas, muitas vezes, em cooperação com o HSI (*Homeland Security Investigations*) e com consulados americanos em outros países, que recebem relatórios detalhados sobre os responsáveis pela propagação de Material de Abuso Sexual Infantil (*Child Sexual Abuse Material* — CSAM) e encaminham à polícia local.

A necessidade de o Brasil adotar uma legislação semelhante à dos Estados Unidos, que imponha aos provedores a obrigação de reportar conteúdos relacionados à exploração sexual infantil e pedofilia, é um ponto crucial no combate aos crimes cibernéticos e na proteção dos direitos fundamentais de crianças e adolescentes.

Contexto brasileiro

Marcello Casal Jr./Agência Brasil



Atualmente, o Brasil possui legislações que criminalizam o abuso e a exploração sexual infantil, como o Estatuto da Criança e do Adolescente (ECA) e a Lei 12.965/2014 (Marco Civil da Internet). No entanto, essas leis não impõem de forma clara uma obrigação direta aos provedores de aplicações, como plataformas de redes sociais, serviços de e-mail e outras empresas digitais, para reportar automaticamente ao governo ou a uma entidade específica qualquer indício de abuso ou exploração sexual infantil detectado em suas plataformas.

Embora o Marco Civil da Internet estabeleça diretrizes gerais sobre a responsabilidade dos provedores de aplicação, ele foca na proteção da privacidade e na remoção de conteúdos ofensivos mediante ordem judicial, sem exigir a comunicação (*report*) compulsória desses casos às autoridades.

Necessidade de uma legislação específica

Uma legislação que exija o reporte obrigatório de conteúdos envolvendo exploração infantil ajudaria a identificar rapidamente criminosos e vítimas. Muitas vezes, as plataformas digitais têm acesso a dados e informações cruciais para investigações policiais, mas, sem uma obrigação legal clara, essas empresas podem não agir de forma eficaz ou rápida o suficiente.

Nos EUA, o CyberTipline do NCMEC tornou-se uma ferramenta essencial para permitir que as empresas reportem automaticamente qualquer detecção de material abusivo. Isso impede que criminosos operem impunemente em plataformas privadas ou menos monitoradas. A adoção de sistemas semelhantes no Brasil daria às autoridades maior capacidade de agir preventivamente e colaborar com autoridades internacionais, especialmente em um contexto em que crimes cibernéticos de exploração infantil frequentemente envolvem redes internacionais.

A responsabilização dos provedores de aplicação no Brasil deve ir além da mera exclusão de conteúdos ilegais mediante ordem judicial. Essas empresas precisam ser vistas como parceiras ativas na proteção de crianças e adolescentes. A imposição de uma obrigação de reporte não é apenas uma questão legal, mas também uma responsabilidade social, considerando o papel crucial dessas plataformas na vida digital contemporânea.

Atualmente, as polícias especializadas em crimes cibernéticos no Brasil, como a Delegacia de Repressão aos Crimes Cibernéticos ou a Delegacia de proteção à criança e ao adolescente, dependem, muitas vezes, de denúncias externas ou de investigações longas e complexas para chegar aos criminosos. Com uma legislação obrigatória de reporte, essas autoridades teriam acesso mais rápido a dados e informações sobre crimes em andamento, permitindo respostas mais ágeis.

Implementação no Brasil

Spacca



Para que essa legislação seja eficaz, o Brasil deveria criar um sistema similar ao CyberTipline do NCMEC, possivelmente administrado por uma entidade independente, como o INCC (Instituto Nacional de Combate ao Cibercrime) ou a SaferNet Brasil, em parceria com as Polícias Civis e a Polícia Federal. As empresas digitais, utilizando tecnologias de detecção, como algoritmos de reconhecimento de padrões de exploração infantil, seriam obrigadas a reportar imediatamente qualquer conteúdo suspeito.

A adesão do Brasil à Convenção de Budapeste, em 2023, que visa à cooperação internacional no combate aos crimes cibernéticos, já é um passo importante, facilitando a troca de informações e a assistência mútua em investigações internacionais. A introdução de uma legislação de reporte obrigatório fortaleceria ainda mais essa posição, alinhando o Brasil às melhores práticas globais no combate à exploração sexual infantil online.

A necessidade de o Brasil criar uma legislação que imponha a obrigação de os provedores de aplicação reportarem conteúdos relacionados à exploração sexual infantil pode ser comparada à previsão legal já existente para instituições financeiras, no que diz respeito à comunicação de atividades suspeitas associadas a fraudes financeiras e à lavagem de dinheiro. Essa comparação revela um paralelo entre as responsabilidades de diferentes setores na prevenção e combate de crimes graves e mostra como um arcabouço normativo semelhante para crimes cibernéticos envolvendo exploração infantil seria igualmente relevante e necessário.

Previsão para instituições financeiras e lavagem de dinheiro

A Lei nº 9.613/1998, que trata dos crimes de “lavagem” ou ocultação de bens, direitos e valores, impõe às instituições financeiras a obrigação de reportar ao Conselho de Controle de Atividades Financeiras (Coaf), ou a outra entidade competente, quaisquer operações financeiras suspeitas de estarem relacionadas a atividades ilícitas, como fraude, corrupção e lavagem de dinheiro.

A prerrogativa do Coaf demonstra que o sigilo bancário pode ser relativizado diante da necessidade de investigação e combate a crimes graves, priorizando o interesse público e a proteção da ordem financeira. Embora o sigilo bancário seja um direito importante para a preservação da privacidade e confidencialidade das informações financeiras dos cidadãos, ele não é absoluto. Em situações em que há fundados indícios de práticas ilícitas, como a ocultação de bens e valores ou a lavagem de dinheiro, a quebra desse sigilo se justifica como uma medida imprescindível para permitir que as autoridades investiguem com eficácia as atividades suspeitas.

Nesse contexto, a legislação brasileira busca equilibrar o direito individual ao sigilo com a necessidade de proteger a sociedade contra crimes que afetam a economia e a integridade das instituições financeiras. A ação do COAF, ao solicitar e compartilhar informações financeiras com outros órgãos competentes, reforça o papel do Estado na prevenção e repressão de crimes financeiros, garantindo que o interesse coletivo prevaleça sobre o direito à confidencialidade em situações de ameaça à ordem pública.



Essa exigência criou um modelo de cooperação entre o setor financeiro e o governo, no qual as instituições financeiras devem monitorar e reportar atividades que, à primeira vista, possam parecer legítimas, mas que podem envolver crimes graves. Além disso, a lei prevê sanções para as instituições que falharem em cumprir essa obrigação, promovendo a proatividade e incentivando a transparência.

Paralelo entre setores: provedores de aplicação e instituições financeiras

A lógica subjacente a essa previsão é semelhante à necessidade de responsabilizar os provedores de aplicação na internet em relação à exploração sexual infantil. Assim como as instituições financeiras têm o dever de identificar e reportar operações suspeitas de fraude ou lavagem de dinheiro, as empresas de tecnologia que hospedam conteúdo online devem ser responsabilizadas por monitorar e reportar atividades ilegais envolvendo crimes contra crianças.

A obrigação das instituições financeiras não as transforma em investigadoras, mas coloca sobre elas o dever de alertar as autoridades competentes, para que as investigações sejam conduzidas. Da mesma forma, os provedores de aplicação não seriam transformados em órgãos de investigação, mas teriam o papel crucial de comunicar às autoridades quando identificassem conteúdos relacionados à exploração infantil, protegendo as vítimas e facilitando a ação policial.

Além disso, assim como as instituições financeiras utilizam ferramentas de análise de dados e monitoramento de transações suspeitas, os provedores de aplicação podem empregar tecnologias, como algoritmos de inteligência artificial, para detectar materiais de abuso sexual infantil. A proatividade dos provedores seria análoga ao comportamento esperado das instituições financeiras: identificar, reportar e colaborar, sem necessidade de intervenção direta na investigação criminal.

Importância da responsabilização e do incentivo ao cumprimento

Assim como a Lei de Lavagem de Dinheiro estabelece sanções para as instituições que falharem em reportar atividades suspeitas, uma legislação voltada ao combate à exploração infantil deveria prever sanções rigorosas para os provedores de aplicação que negligenciarem a obrigação de comunicar às autoridades competentes qualquer atividade relacionada a esse crime. Essa responsabilização é essencial para garantir que as plataformas digitais ajam de forma eficaz e colaborativa no combate à exploração sexual infantil.

O incentivo ao cumprimento dessas obrigações por parte dos provedores de aplicação deve ir além da imposição de sanções, podendo incluir a criação de programas de certificação de boas práticas para as empresas que adotarem políticas mais rigorosas de combate à exploração infantil. Esses mecanismos de compliance e a colaboração com as autoridades são fundamentais para criar um ambiente digital mais seguro.

Cooperação internacional e integração de dados

Outro ponto crucial, tanto na previsão de reporte de crimes financeiros quanto no combate à exploração infantil online, é a necessidade de cooperação internacional. No caso da lavagem de dinheiro, as atividades fraudulentas geralmente têm natureza transnacional, exigindo colaboração entre diferentes autoridades financeiras e policiais de diversos países. O mesmo ocorre com a exploração sexual infantil, onde redes de pedofilia e crimes cibernéticos não respeitam fronteiras nacionais.

O Brasil já faz parte de acordos internacionais de cooperação para o combate a crimes cibernéticos, como a Convenção de Budapeste. Ao estabelecer uma legislação que imponha aos provedores de aplicação o dever de reportar atividades relacionadas à exploração sexual infantil, o Brasil poderia integrar esses dados em redes globais de combate a esses crimes, facilitando a troca de informações com outras nações e agências internacionais. Essa integração de dados ajudaria a identificar redes de exploração que operam em múltiplos países, permitindo uma ação coordenada e mais eficaz.

A comparação entre a obrigatoriedade de reporte de atividades suspeitas por instituições financeiras e a necessidade de uma legislação similar para provedores de aplicação no combate à exploração sexual infantil mostra como o Brasil pode avançar significativamente em sua capacidade de lidar com crimes cibernéticos graves. A responsabilidade compartilhada entre setores-chave, como o financeiro e o tecnológico, pode contribuir para a construção de uma rede de proteção eficaz contra criminosos que utilizam a internet para praticar abusos, promovendo uma sociedade mais segura e garantindo a proteção de crianças e adolescentes.

É necessário e urgente, portanto, criar uma legislação brasileira que obrigue os provedores de aplicação a reportarem automaticamente quaisquer conteúdos relacionados à exploração sexual infantil. Esse passo é essencial para modernizar o combate aos crimes cibernéticos, garantindo não apenas a proteção de crianças e adolescentes, mas também colocando o Brasil em uma posição de liderança no enfrentamento desses crimes em âmbito global, reforçando a cooperação com outros países e autoridades internacionais.

Fonte: <https://conjur.jumps.com.br/2024-out-27/responsabilidade-dos-provedores-de-internet-no-combate-a-exploracao-sexual-infantil/>