PROJETO DE LEI Nº , DE 2024

(Da Sra. Deputada Federal LAURA CARNEIRO)

Altera o art. 21 da Lei n° 12.965, de 2014, Marco Civil da Internet para obrigar os provedores de aplicação a tomar medidas imediatas e eficazes para tornar indisponíveis outros URLs que contenham ou links que apontem para o material já identificado como infringente.

O Congresso Nacional decreta:

Art. 1º Esta Lei altera o art. 21 da Lei n° 12.965, de 2014, Marco Civil da Internet, para obrigar os provedores de aplicação a tomar medidas imediatas e eficazes para tornar indisponíveis outros URLs que contenham ou apontem para o material já identificado como infringente.

Art. 2° O atual parágrafo único do art. 21 da Lei n° 12.965, de 2014, passa a vigorar como § 1°, sendo acrescido ao artigo o seguinte § 2°:

Art.
21. ....
.....

§ 1° .....

§ 2° Recebida a primeira notificação, o provedor de aplicação deve tomar medidas imediatas e eficazes para tornar indisponíveis outros URLs que contenham ou links que apontem para o material já identificado como infringente. (NR)

Art. 3° Esta lei entra em vigor na data da publicação.

JUSTIFICAÇÃO

A atual redação do art. 21 do Marco Civil da Internet requer que o provedor de aplicações remova conteúdo que viole a privacidade somente após notificação específica para cada URL, o que torna a legislação ineficaz para reparar danos causados à vítima de divulgação não autorizada de conteúdo íntimo.

A disseminação rápida e ampla de conteúdo ilegal na internet pode causar danos irreparáveis a indivíduos afetados, especialmente a mulheres e crianças em casos de divulgação de imagens ou vídeos de sexo e nudez não-autorizados. Para tratar deste problema de forma mais eficiente, jurisdições de vários países já substituíram a prática do *"notice and take down*" pela regra do *"notice and stay down*", onde o provedor de aplicação é obrigado a manter o conteúdo removido, prevenindo a publicação das mesmas imagens ou vídeos infringentes em outro endereço virtual.

Em artigo publicado na Agenda Brasileira sobre Direito Digital, são citados exemplos de decisões tomadas por diferentes países, nos quais provedores de aplicação são obrigados a prevenir a disseminação de um conteúdo ilícito específico, após a realização de uma primeira notificação. A saber:

> Em diversas ocasiões, a Corte Europeia de Justiça já afirmou ser incompatível com a Carta Europeia de Direitos Humanos a realização de monitoramento prévio de conteúdo sobre tudo o que os usuários publicam na internet. Em casos relevantes, no entanto, fez uma diferenciação entre monitoramento geral e específico.
>
> De acordo com a Corte Europeia de Justiça, a proibição de monitoramento geral impede a criação de leis que, para impedir ilícitos futuros, obriguem as plataformas a instalarem um sistema: a) que filtre informação armazenada em seus servidores; b) como uma medida preventiva; c) de maneira geral e indiscriminada em relação a todos os usuários; d) por um período indeterminado; e) que tenha

> o custo exclusivamente suportado pela empresa; e f) capaz de identificar arquivos contendo músicas ou vídeos.
>
> Não obstante, a mesma Corte admite que, para proibir a prática de ilícitos futuros, pode ser imposto monitoramento voltado a prevenir infrações: a) do mesmo tipo; b) praticados pelo mesmo autor previamente identificado; e c) relacionado às mesmas marcas.
>
> Entre outros casos (FROSIO, 2017), há ainda exemplos de Cortes na França, na Alemanha e na Inglaterra que determinaram aos aplicativos de busca a obrigação de monitorar e desindexar links que remetessem a imagens já declaradas previamente ilícitas, tais como as de Max Mosley, ex-presidente da Federação Internacional de Automobilismo, tendo relações sexuais. Na Inglaterra, a ação movida por Mosley teve como suporte a Lei de Proteção de Dados Pessoais, afirmando a Corte ser de conhecimento geral a existência de tecnologia que permitiria o Google, sem grandes esforços nem custos relevantes, monitorar e reduzir o acesso a tais imagens.
>
> Na Alemanha, a Corte de Hamburgo destacou que impor àquele que tem a privacidade violada o dever de notificar o provedor de busca e indicar a correspondente URL à cada nova publicação das imagens ofensivas revela-se como um mecanismo inadequado e insuficiente de proteção à privacidade, pois o ônus de monitorar permanentemente o específico conteúdo ilícito na internet seria imposto à parte mais fraca da relação e a que está mais longe de dispor dos mecanismos tecnológicos adequados para proteger o direito à privacidade. Sobre a capacidade do Google de monitorar e bloquear o acesso às imagens, a Corte mencionou o uso de aplicativos atualmente comuns no mercado como o PhotoDNA, iWatch e o Content-ID. [1]

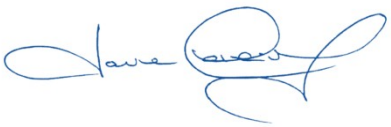
Considerado o quadro, a alteração proposta busca assegurar uma abordagem mais robusta e rápida para combater a propagação de conteúdo ilícito de natureza sexual, alinhando a legislação às decisões recentes tomadas por cortes e leis de outros países democráticos bem como ao princípio de proteção da privacidade e da dignidade humana, em especial de mulheres e crianças.

Trata-se de medida intermediária entre a criação de um dever de monitoramento geral e prévio dos conteúdos publicados por todos os usuários e a regra hoje existente, a qual considero completamente ineficaz e aquém do que é possível realizar com a atual tecnologia atualmente disponível.

[1] SANKIEVICZ, Alexandre. O caminho do meio entre a imunidade e a responsabilidade das plataformas pelo conteúdo publicado por terceiros. ARAÚJO. José Evande Carvalho (org). AGENDA BRASILEIRA: economia digital. Câmara dos Deputados, Ano 4, 2023, n° 6. P. 217-219.

Ante o exposto, peço o apoio dos meus pares para aprovar o projeto de lei.

Sala das Sessões, em 17 de maio de 2024.



Deputada Federal LAURA CARNEIRO

2024-5565