Brasil deve atualizar legislação contra hackers, dizem advogados

As ameaças digitais cresceram quase 400% em 2020 em relação a 2019, segundo a Cybersecurity Intelligence. Cada vez mais os ataques têm visado organizações públicas, como aconteceu no Superior Tribunal de Justiça e Tribunal Superior Eleitoral. Para advogados, o Brasil deve atualizar a legislação, visando criar as condições jurídicas que permitam às autoridades policiais agirem contra os *hackers* internacionais, como já fazem outros países.

Reprodução

Brasil deve atualizar legislação contra ataques de *hackers*, dizem advogados
EReprodução

Para o advogado **Solano de Camargo**, especialista em Direito Digital e sócio fundador da banca LBCA, a Lei Carolina Dieckmann (Lei 12.737/2012) e o Marco Civil da Internet (Lei 12.965/2014) não dão conta de *hackers* de fora do país.

"O contra-ataque policial (*hackback*) contra hackers internacionais é uma solução para os desafios crescentes dos crimes cibernéticos, potencializados pelos desafios do anonimato, da criptografia e da computação na nuvem. Ao implantar um sistema legal e técnico que permita o *hackback*, as autoridades poderão acessar computadores de criminosos localizados no exterior e colher provas na origem, contornando a criptografia dos dados. Mas para isso, é fundamental a atualização das leis brasileiras, que hoje não diferenciam um ataque hacker de um contra-ataque iniciado pelas autoridades, qualificando ambos como um mesmo ato ilícito cibernético: o crime de invasão de dispositivo informático", diz Camargo.

Após as autoridades policiais conseguirem o acesso remoto a um computador localizado no exterior para a prática de crimes cibernéticos, aponta o advogado, a experiência internacional mostra que é possível a localização dos responsáveis pelo sinal de GPS e sua identificação por voz e imagem pelo microfone e câmeras de vídeo de seus próprios computadores.

"Também é possível, como fazem hoje as autoridades dos EUA, França e Suíça, copiar remotamente os dados relevantes do hacker para fins de prova em uma investigação criminal, que podem ser compartilhados com as autoridades de outros países".

Outra medida que o advogado destaca como útil já é utilizada por policiais estrangeiros: tornar inacessível o equipamento ou os dados obtidos ilicitamente, após invadirem a estrutura dos hackers, mesmo que esteja localizada no exterior.

Para Camargo, a experiência internacional tem mostrado que essas medidas permitem alcançar resultados muito relevantes como, por exemplo, a desativação de infraestruturas de *botnet* (rede de computadores zumbis controlados por um ou mais hackers) ou a criptografia de dados furtados, como informações bancárias ou imagens de pedofilia.

Estela Aranha, advogada e presidente da Comissão de Proteção de Dados e Privacidade da seccional do Rio de Janeiro da OAB, avalia ser necessária a atualização da legislação brasileira em relação aos crimes cibernéticos, até porque esse é um dos principais riscos hoje que empresas e governos têm de enfrentar. Porém, "a aposta em majoração das penas isoladamente não é a resposta adequada para resolver a ameaça de crimes cibernéticos", declara.

"A prevenção é central nesse debate é nós não temos uma cultura de segurança de informação, tampouco de proteção de dados pessoais, nem no setor público nem no privado de modo geral. Essas questões são negligenciadas hoje e só lembradas quando ocorrem grandes vazamentos. Temos ainda a falta de capacidade para investigar e encontrar os responsáveis pelos crimes cibernéticos. A sensação de impunidade vem muito mais de não se chegar aos autores dos crimes, da dificuldade de investigação desses crimes", destaca Estela.

Já **Marco Antonio Sabino**, sócio da área de Mídia e Internet do Mannrich e Vasconcelos Advogados, opina que o grande problema está na fiscalização e na especialização dos órgãos públicos, e não na legislação. Segundo ele, é preciso melhorar os aparatos públicos de cibersegurança (polícias, Ministério Público e varas especializadas).

Sabino lembra que o Código Penal já prevê o crime de invasão de dispositivo informático, contudo, ressalta que a pena é baixa. "Na verdade, como esses ataques podem partir de fora do território nacional, penso que o caso é de tratados e cooperação para combater esses criminosos. O Código Penal prevê até causas de aumento de pena dependendo do agente atacado e das informações violadas."

Nessa linha, **André Damiani**, criminalista especializado em Direito Penal Econômico e sócio fundador do Damiani Sociedade de Advogados, analisa que a principal solução não está em uma atualização legislativa, mas em um amplo enfoque para as práticas preventivas. "As organizações públicas, bem como as empresas que podem ser alvo de ataques de hackers devem implementar políticas de governança de dados para fortalecer os sistemas de segurança intrínsecos a elas e se resguardar de ataques de sequestro de dados."

Entre outras medidas, Damiani sugere a realização de *backups*; utilização de redes *wi-fi* estáveis e

seguras; instalação de antivírus e *antimalwares*; elaboração de uma política de privacidade e regras de segurança; e tentativas de ataques por "hackers do bem" com uma determinada frequência, para medir o nível de segurança.

"Porém, uma das principais providências a serem tomadas pelas empresas e órgãos públicos é o treinamento dos colaboradores e conscientização sobre os riscos de *phishing*, *ransomware* e demais estratégias utilizadas pelos hackers", acrescenta **Blanca Albuquerque**, sócia de Damiani e especialista em proteção de dados pessoais pelo Data Privacy Brasil. "Além disso, as organizações devem ter uma estratégia muito bem delimitada para enfrentar casos de incidentes de segurança, definindo o que fazer desde as primeiras horas e como os colaboradores devem ser mobilizados nessas ocasiões, evitando pânico e desorganização em momentos importantes e decisivos", afirma.

Esforço internacional
Wilson Sales Belchior, sócio do Rocha, Marinho E Sales Advogados e conselheiro federal da OAB, aponta que a Organização dos Estados Americanos concluiu em relatório de 2020 sobre a capacidade brasileira de cibersegurança que a legislação sobre o tema continua em desenvolvimento. "Recomendou, assim, abordagem específica às ameaças cibernéticas à propriedade intelectual, expansão dos mecanismos de cooperação e designação de órgão para monitorar o cumprimento das normas e regulamentos a respeito do tema."

A própria estratégia nacional (Decreto 10.222/2020), diz Belchior, reconhece a importância de aprimorar o arcabouço legal, incluindo entre as ações estratégicas abordagem de temas ausentes, novas tipificações de crimes cibernéticos e elaboração de anteprojeto de lei tratando da segurança cibernética.

"Sem dúvidas, existe espaço para aperfeiçoamento normativo nessa área, contudo precisam ser mencionados avanços importantes. Na Lei Geral de Proteção de Dados (Lei 13.709/2018), é destacável o capítulo referente à segurança e boas práticas, bem como a competência da Autoridade Nacional de Proteção de Dados para determinar padrões técnicos de segurança voltados a proteção de dados pessoais. No Poder Judiciário, o Conselho Nacional de Justiça instituiu o Comitê de Segurança Cibernética, responsável, dentre outros aspectos, por apresentar protocolos de prevenção e investigação, estratégia da segurança cibernética e da informação, além de propor norma para criação de Centro de Tratamento de Incidentes", afirma o advogado.

Luiz Felipe Rosa Ramos, co-head de Proteção de Dados da Advocacia José Del Chiaro, diz que o Brasil demonstrou, nos últimos anos, capacidade de garantir segurança cibernética durante a realização de eventos internacionais.

No entanto, ressalta, a posição global do país nesse quesito segundo a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) ainda é baixa (70º lugar) e os novos desafios com uma economia digitalizada são cada vez maiores.

"Algumas recomendações, endossadas pela OCDE, são: (i) estabelecer um processo periódico de revisão e aprimoramento das leis de segurança cibernética, dado o caráter dinâmico das ameaças e (ii) estabelecer programas de capacitação institucional para juízes, promotores e pessoal policial com vistas a adquirir novas competências necessárias para atuar em questões cibernéticas. De modo geral, o Brasil ainda precisa realizar um esforço amplo de conscientização sobre o tema da segurança cibernética, o que

tende a ser estimulado com a entrada em vigor da LGPD", destaca Ramos.

Date Created
16/01/2021