PODER EXECUTIVO

Uma agência para combater cibercrimes

Governo prepara projeto de lei para criar órgão regulador que será responsável pela política de segurança digital do país

» HENRIQUE LESSA

Crimes virtuais causam um prejuízo de US$ 10,5 trilhões (R$ 53 trilhões, aproximadamente) ao ano no mundo, o equivalente a quase cinco vezes o Produto Interno Bruto (PIB) brasileiro de 2023. O governo do presidente Luiz Inácio Lula da Silva (PT) estabeleceu como prioridade o combate a esse tipo de delito e, ainda neste ano, espera ver funcionando a Agência Nacional de Cibersegurança. O comitê que deve definir o modelo da entidade que será responsável por cuidar da implementação da política nacional para a segurança digital terá sua primeira reunião na próxima quarta-feira.

"É a quarta maior preocupação global dos próximos dois anos. Há um relatório da Cybersecurity Ventures que fala que os custos globais com o cibercrime podem chegar a US$ 10,5 trilhões por ano. Esse valor é maior do que todos os danos causados por desastres naturais, e uma modalidade de crime mais lucrativa que todo o comércio de drogas ilegais", destacou ao **Correio** o advogado especialista em cibersegurança e diretor da Federação das Indústrias de São Paulo (Fiesp) Rony Vainzof.

No lançamento do Plano Nacional de Cibersegurança (PNCiber), no fim de dezembro, o governo Lula apontou a urgência e relevância do tema, posto que o Brasil é o terceiro país com maior número de ataques cibernéticos no mundo.

A criação de um organismo de segurança digital vem sendo discutida dentro do governo federal, pelo menos, desde 2013, quando o vazamento divulgado pelo Wikileaks mostrou que os Estados Unidos grampearam telefones da então presidente Dilma Rousseff e de diretores da Petrobras. Mas, apesar da urgência, só neste mês é que vai acontecer a primeira reunião do CNCiber.

O colegiado, coordenado pelo Gabinete de Segurança Institucional (GSI) da Presidência, é composto por 25 membros titulares, com representantes de 13 ministérios, da Agência Nacional de Telecomunicações (Anatel), do Banco Central, de instituições científicas, de empresários do setor de cibersegurança e da sociedade civil.

Apesar de ainda não se ter a formatação final — se será mais uma agência reguladora, por exemplo —, especialistas apontam que essa é a modelagem mais provável. "Acho que o caminho é ter uma agência, sim, e essa agência tem um papel de estruturar as diretrizes para elevar o nível de maturidade no Brasil, cuidar de infraestruturas críticas, isso é superrelevante", aponta Vainzof.

No Congresso, o tema não deve tramitar de forma tão pacífica. A oposição dá sinais de que tentará barrar a criação do órgão responsável pelo enfrentamento ao crime digital. Correligionários do ex-presidente Jair Bolsonaro (PL) dizem que só vão se posicionar depois do envio do projeto de lei, mas, reservadamente, demonstram desconfiança com a possibilidade de a agência se tornar um "cabide de empregos" para aliados do governo ou, pior, agir para regular a utilização das redes, principal ferramenta de comunicação da direita mais radical.

Luana Tavares, CEO do Instituto Nacional de Combate ao Cibercrime (INCC), disse ao **Correio** que, mesmo reconhecendo o receio de alguns parlamentares quanto à agência atuar na regulação de plataformas, esse não é o debate importante no momento. Para ela, não se pode perder de vista uma agenda que considera fundamental.

"A discussão no Congresso faz parte do jogo democrático, o debate político vai ter que acontecer. Mas o principal é a gente entender o objetivo dessa agência. O que precisamos saber é o custo para o país em não ter essa estrutura. Por isso, devemos olhar as experiências internacionais", recomenda a especialista.

Tavares aponta para a necessidade de endurecer a lei penal sobre crimes digitais. "A gente precisa de um arcabouço legal que especifique melhor esse tipo de crime. Os crimes digitais vêm sendo tratados por analogia no Código Penal. Existem várias formas de crimes cibernéticos que não estão previstos. Quando você fala no ambiente digital, os desdobramentos dos crimes, hoje, transcendem o alcance da lei penal", defende.

Outro desafio do governo na implementação da agência é a resistência da Polícia Federal, que questiona a viabilidade e o orçamento do órgão. Desde o início do governo Lula, integrantes da corporação deixam claro a disputa pelo espaço institucional ocupado pelo GSI.

A outra pedra no caminho da criação da agência, mesmo após a aprovação do projeto de lei no Congresso, é encontrar espaço no Orçamento da União para custear o novo órgão regulador. Técnicos estimam que o governo gastará, pelo menos, R$ 600 milhões por ano.

GSI à frente

A coordenação das estratégias do governo está a cargo do GSI, comandado pelo general Marcos Antônio Amaro dos Santos. Além do tema ser uma preocupação constante das empresas — que têm a maior parte dos seus sistemas na nuvem —, a cibersegurança tem um papel fundamental na estratégia de defesa nacional.

"Indicadores internacionais demonstram que todos os países estão sofrendo com o mesmo problema. Essa iniciativa do governo, do GSI, é superimportante, visto que o Brasil tem tido um aumento grande nos crimes cibernéticos, e isso afeta o crescimento do país, a vida das pessoas", argumenta Luana Tavares.

Um ponto prioritário para o GSI é a possibilidade de o país sofrer ataques contra suas infraestruturas críticas, como plantas de energia ou linhas de transmissão. Fontes no órgão, reservadamente, ressaltam que eventos como o apagão de 2023, causado por uma sobrecarga que atingiu a todos os estados, exceto Roraima, poderia se repetir por um ataque cibernético se medidas de cibersegurança adequadas forem negligenciadas.

Um exemplo dessa ameaça se deu em 2021, quando criminosos sequestraram os sistemas do maior oleoduto dos Estados Unidos, da empresa Colonial. O ataque de hackers à companhia, responsável por 45% do abastecimento de diesel, gasolina e querosene de aviação da Costa Leste do país, fez a Casa Branca decretar estado de emergência.

Números e expectativas

Ataques em 2022 (Estimativa)

103 bilhões de invasões de hackers no Brasil (Fonte: GSI)

Prejuízo dos crimes digitais

US$ 10,5 trilhões/ano no mundo (Fonte: Cybersecurity Ventures)

Expectativa dos líderes empresariais*:

86% acreditam que é "provável" uma catástrofe cibernética de longo alcance

Nos próximos dois anos, a inteligência artificial trará mais vantagens para:

Hackers: 55,9%
Hackers e Segurança: 35,1 %
Segurança: 8,9%

A regulação cibernética e de privacidade reduz o risco de ataques?

Sim: 60,4%
Não: 18,8%
(*Fonte: Global Cybersecurity Outlook)

Falhas, no Brasil, da política de cibersegurança

Governo:

- Resposta a incidentes
- Proteção de infraestrutura crítica

Sociedade:

- Cultura da população no uso de redes sociais

Tecnologias:

- Controles técnicos de segurança
- Controles criptográficos

(Fonte: Centro Global de Capacidade de Segurança Cibernética/GCSCC — Oxford)

Brasil precisa avançar mais nas tecnologias

Segundo o Global Cyber Index — uma pesquisa feita com dados do Banco Interamericano de Desenvolvimento (BID) —, entre 183 países analisados, o Brasil está na 18ª colocação em segurança digital. Mas, apesar da boa posição do país nesse índice, outros estudos indicam que ainda há muito a ser feito para qualificar o país, que é o que mais sofre ataques cibernéticos em toda a América Latina e figura como terceiro colocado no mundo.

O Gabinete de Segurança Institucional (GSI), que coordena o processo de implementação da Política Nacional de Cibersegurança, encomendou dois estudos: o primeiro, de análise da situação brasileira, e outro, de comparação com experiências internacionais.

Um desses estudos, solicitado ao BID, aponta que o país ainda está em uma posição intermediária em comparação com quem já está na terceira geração em termos de prevenção e adoção de medidas de cibersegurança contra ataques a negócios, infraestruturas críticas do serviço público e de instituições, e na defesa da democracia.

Apesar de avanços no marco legal com Lei Geral de Proteção de Dados (LGPD), o país é, entre as grandes economias, um dos menos preparados para esse tipo de ataque. Com dados de 2022, o país corre o risco de se tornar um porto seguro para cibercriminosos de todo o planeta. Um modelo internacional apontado como referência ao projeto brasileiro é o da União Europeia, que tem uma agência dedicada ao assunto há mais de 20 anos.

Em outro estudo, encomendado pelo GSI à Universidade de Oxford, do Reino Unido, a resiliência brasileira a ataques cibernéticos é apontada com mediana. A instituição aponta atrasos na comparação com o mesmo estudo feito em 2020, sobre as capacidades de resposta a incidentes de ataques, à proteção das infraestruturas críticas do país, à implementação de controles técnicos de segurança e a controles criptográficos nas organizações.

A centralidade do tema trouxe o assunto para o Fórum Econômico Mundial deste ano, na Suíça, com um relatório — o *Global Cybersecurity Outlook* — que mostra que 86% dos líderes empresariais veem como provável uma "catástrofe" cibernética de "longo alcance" nos próximos dois anos. Mas os empresários também reconhecem que a regulação feita pelos governos está trazendo mais segurança ao ambiente de negócios.

Segundo o estudo, há uma grande diferença na maturidade de cibersegurança entre as grandes companhias e as médias e pequenas empresas, mas, mesmo as grandes podem ficar vulneráveis pelas fragilidades de parceiros ou fornecedores.

Para Luana Tavares, CEO da ONG Instituto Nacional de Combate ao Cibercrime (INCC), essa diferença de maturidade no Brasil é ainda mais relevante. "Estudos indicam que, quando uma pequena ou média empresa sofre um ataque cibernético, muitas acabam fechando as portas em até seis meses depois do ataque. E são as pequenas e médias empresas — 99% das companhias no país — que geram 70% dos empregos formais", aponta. (**HL**)