MAIS BARREIRAS CONTRA CIBERATAQUES

Legislação brasileira focada em segurança de dados avança, mas aparelhos conectados à internet ainda continuam vulneráveis

Sarah Schmidt

Há boas razões para temer que informações pessoais ou de empresas vazem do celular ou do computador e sejam usadas sem o controle de seus donos. No Brasil, a chamada segurança cibernética ainda precisa melhorar, embora a legislação brasileira esteja avançando, com a participação de especialistas de universidades, empresas e centros de pesquisa. Definida como um conjunto de ações para proteger máquinas e pessoas contra invasões, a segurança cibernética implica aprimoramentos contínuos no campo da regulação, tecnologia e processos por parte de governos, usuários e setor privado.

O engenheiro eletricista Edmar Gurjão, da Universidade Federal de Campina Grande (UFCG), na Paraíba, deve apresentar em agosto à Agência Nacional de Telecomunicações (Anatel), em Brasília, propostas de medidas legais para reduzir a vulnerabilidade da tecnologia 5G, a internet de quinta geração, que começa a ser implantada no Brasil. Gurjão lidera um estudo que reúne 52 pesquisadores brasileiros cujo objetivo é oferecer subsídios para que a agência avalie a necessidade de criar medidas legais específicas para esse tipo de tecnologia. Uma das recomendações que pretende fazer é que a Anatel exija certificação de fábrica dos softwares instalados nos dispositivos aptos a funcionar com 5G, garantindo que os parâmetros de segurança estejam atualizados. "A alta velocidade e a conexão entre os aparelhos 5G expõem mais os usuários a ataques cibernéticos", diz o pesquisador.

Há muito por fazer. Entre os países da América Latina, as redes e os aparelhos ligados à internet no Brasil estão entre os mais vulneráveis. O país sofreu 103 bilhões de tentativas de ataques cibernéticos em 2022, atrás apenas do México (com 187 bilhões), segundo levantamento da empresa norte-americana de cibersegurança Fortinet. Em comparação com 2021, o número de ataques no país aumentou 16%. Mundialmente, de acordo com esse mapeamento, 82% dos ataques que tentaram roubar dinheiro de usuários e instituições usaram programas de ransomware, que sequestram dados e contas, só devolvidos aos seus donos após pagamento de um resgate.

Mesmo assim, de 2018 para 2020, o país saltou da 70ª posição para a 18ª no mais recente Índice Global de Segurança Cibernética, elaborado pela União Internacional de Telecomunicações (ITU), que avalia as ações dos países mais bem preparados para lidar com ataques de hackers. Provavelmente o avanço se deve aos aprimoramentos da legislação, um dos itens avaliados pela ITU, no qual o país obteve a nota máxima. Embora sejam fundamentais, apenas instrumentos legais não bastam, advertem os especialistas.

"O desafio principal do Brasil não é ter boas medidas regulatórias, mas implementá-las e monitorá-las", diz a advogada Ana Luíza Calil, doutoranda em direito administrativo na Universidade de São Paulo (USP). Em artigo publicado em maio de 2022 na revista científica *International Cybersecurity Law Review*, ela e o advogado Roberto Carapeto, da Universidade de Nagoya, no Japão, analisaram a legislação brasileira e de outros quatro países da América Latina: Argentina, Chile, Colômbia e México. Segundo eles, todos têm criado seus próprios mecanismos legais para reforçar a segurança cibernética, mas estão em estágios diferentes. "Entre os cinco países, o Brasil tem o conjunto de regulações mais avançado, seguido pelo Chile", observa Calil. Segundo ela, o México ainda está em fase inicial.

O Marco Civil da Internet, aprovado em abril de 2014, abriu caminho para outras normas importantes. Entre as mais recentes, destaca-se a Lei Geral de Proteção de Dados (LGPD), em vigor desde agosto de 2020, que regulamenta o tratamento de dados pessoais (por exemplo, nome, sobrenome, CPF, RG, endereço residencial e identificação do computador). "É a única no Brasil que prevê objetivamente multa por vazamento e armazenamento inadequado de dados pessoais", afirma o engenheiro da computação Roberto Gallo, diretor da empresa de criptografia Kryptus e

FOTOMONTAGEM LÉO RAMOS CHAVES / REVISTA PESQUISA FAPESP

presidente da Associação Brasileira das Indústrias de Materiais de Defesa e Segurança (Abimde).

"A LGPD deixa claro que é preciso proteger os dados pessoais porque a empresa responsável por eles vai responder pelos vazamentos", comenta Gallo. "Seria importante expandi-la ou criar uma legislação para proteger outros tipos de dados, como os comerciais, industriais e dos sistemas críticos."

Um caminho importante para o setor avançar, além de contar com regulamentações estruturadas, é garantir investimentos das empresas em segurança da informação. Em 2020, Gallo estimou que, no Brasil, eles não chegavam a 4% do orçamento da área de tecnologia da informação das companhias, enquanto em países mais desenvolvidos o valor era de 10% a 15%. Segundo ele, a Abimde ainda não tem dados atualizados sobre essa média no país, mas estima que não houve grandes mudanças. Segundo projeções da consultoria de inteligência de mercado norte-americana IDC, os gastos com soluções de segurança no Brasil devem atingir US$ 1,3 bilhão em 2023, 13% a mais que o ano anterior.

Outro marco legislativo importante é a Estratégia Nacional de Segurança Cibernética (E-Ciber), aprovada como decreto em fevereiro de 2020, com diretrizes e ações estratégicas de segurança cibernética, como incentivo à pesquisa. "A Estratégia Nacional procura harmonizar os objetivos de quem lida com cibersegurança, mas falta clareza sobre as atribuições de cada participante e as formas de monitoramento das ações, incluindo a interação da União com estados e municípios", comenta Calil.

Mesmo assim, ela ressalta os desdobramentos desse plano, como uma resolução do Banco Central, de abril de 2021, com diretrizes de segurança cibernética para instituições financeiras. Em junho daquele ano, o Conselho Nacional de Justiça (CNJ) divulgou normas de cibersegurança para os órgãos do Poder Judiciário para proteger as informações de mais de 77 milhões de processos digitalizados.

A Estratégia vigora até o final de 2023. Consultado sobre os planos de atualização do decreto, o Gabinete de Segurança Institucional (GSI) da Presidência da República, responsável pela elaboração do documento, observou, em nota enviada a *Pesquisa FAPESP*, que tem avaliado desde 2022 tópicos que precisam ser aprimorados.

O órgão informou que analisará também contribuições "da comunidade de segurança cibernética e das que resultarem de consulta pública", indicando que, assim como na formulação da Estratégia atual, apresentará o projeto do documento para avaliação prévia da sociedade. Não revelou, porém, quando isso deve ser feito.

Gurjão, da UFCG, ressalta a importância de criar um centro unificado para registros de incidentes cibernéticos, previsto na Estratégia. A seu ver, esse centro poderia permitir ações conjuntas mais rápidas de defesa entre instituições responsáveis por serviços essenciais como fornecimento de água, energia, telecomunicações e segurança pública, em caso de ataques.

"É importante formar uma coalizão com os diversos setores do governo e da sociedade civil, já que a segurança cibernética lida ao mesmo tempo com uma ameaça difusa e híbrida, que pode atingir qualquer pessoa, empresa ou instituição", diz Raquel Jorge de Oliveira, analista

PARA NAVEGAR COM MAIS SEGURANÇA

Algumas recomendações para uso de dispositivos com acesso à internet

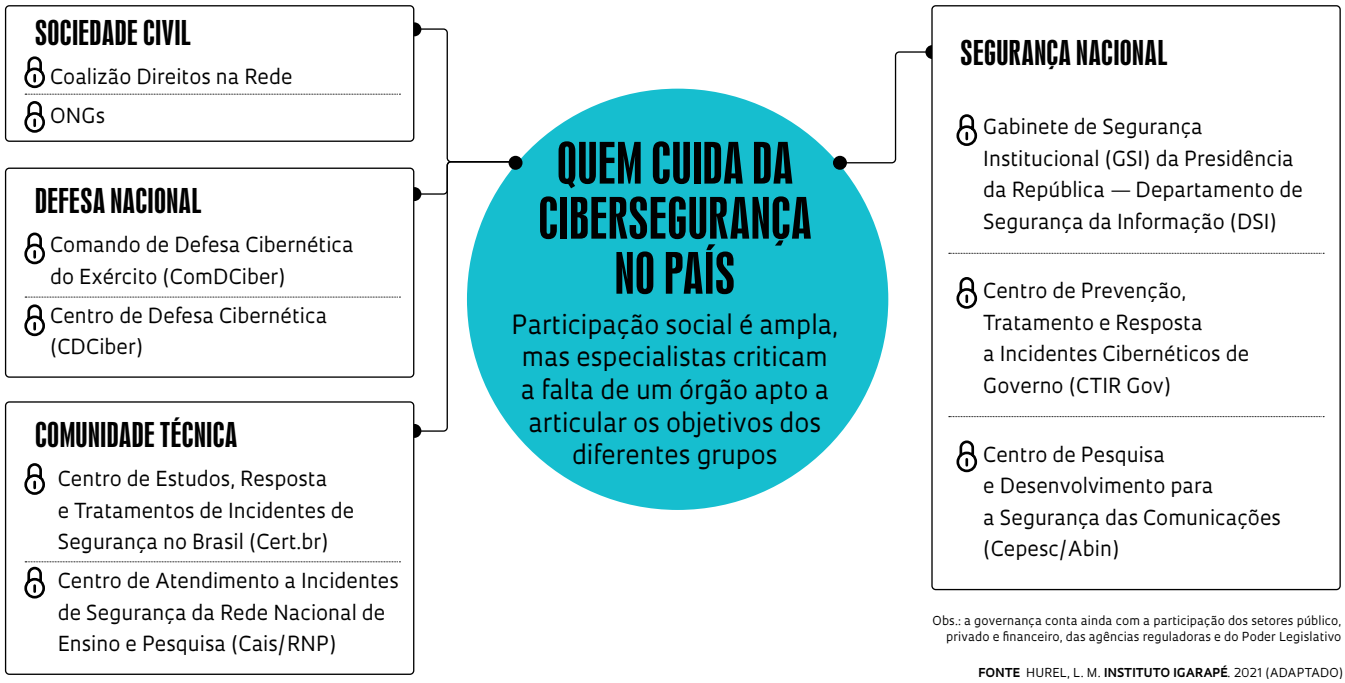
NO SEU CELULAR

- Configure uma senha forte para bloquear a tela inicial
- Desabilite funções com a tela bloqueada, como a visualização de mensagens
- Quando trocar de aparelho, apague todos os dados e desvincule-o de contas bancárias e outros aplicativos
- Altere o código do pin padrão que vem no seu chip
- Crie uma senha para o seu chip
- Lembre-se de guardar o número Imei (identidade internacional de equipamento móvel), que permite bloquear e desbloquear o celular

EM QUALQUER DISPOSITIVO COM ACESSO À INTERNET

- Não clique em qualquer link que receber. Entre em contato com a pessoa que o enviou, por outro meio, para checar se foi ela quem mandou
- Não publique seus dados pessoais em redes sociais
- Nunca responda a mensagens ou ligações que solicitem seus dados pessoais, bancários ou senhas
- Use senhas distintas para aplicativos diferentes
- Não encaminhe códigos de acesso recebidos em mensagens para terceiros
- Não reencaminhe mensagens de origem desconhecida ou com links duvidosos
- Não acesse contas de banco quando estiver logado em Wi-Fi público

FONTE CAMPANHA #FIQUE ESPERTO DA ASSOCIAÇÃO BRASILEIRA DE EMPRESAS DE INTERNET



Obs.: a governança conta ainda com a participação dos setores público, privado e financeiro, das agências reguladoras e do Poder Legislativo

FONTE HUREL, L. M. **INSTITUTO IGARAPÉ**. 2021 (ADAPTADO)

de inteligência na startup de cibersegurança Harpia Tech, do Rio de Janeiro.

Em seu mestrado, concluído em 2021 na Universidade de Brasília (UnB), ela comparou a política brasileira com a de quatro países europeus – Finlândia, Suécia, Dinamarca e Noruega – considerados referências internacionais em cibersegurança. Nos quatro, há um diálogo permanente entre as instituições e os usuários de internet, o que, segundo ela, não ocorre no Brasil. Oliveira detalhou as conclusões em um artigo publicado em fevereiro de 2022 na revista *Brasiliana: Journal for Brazilian Studies*.

"A legislação sobre cibersegurança no Brasil prevê a interação entre setores do governo e a sociedade civil, mas sempre sob o comando do GSI ou do Ministério da Defesa, sem estruturas permanentes de coordenação e de interação entre órgãos do governo e os usuários", diz Oliveira.

Graduada em relações internacionais, Louise Marie Hurel, mestranda na London School of Economics, no Reino Unido, tem uma visão semelhante. Em uma análise publicada pelo Instituto Igarapé, instituição não governamental do Rio de Janeiro dedicada à segurança climática e digital, ela comentou: "Por mais que o GSI já desempenhe a função de coordenação e facilitação na administração pública federal, sua relação com a sociedade civil permanece frágil, com grupos frequentemente apontando a falta de transparência e militarização da agenda do Departamento de Segurança da Informação do GSI".

Questionado sobre essa militarização, o GSI informou, em nota, que a defesa cibernética nacional está, de fato, entre as competências do Ministério da Defesa. Mas a segurança cibernética do país, segundo o órgão, "compete majoritariamente a organizações civis". Como instituições civis importantes nessa área, o GSI cita o Centro de Atendimento a Incidentes de Segurança (Cais) da Rede Nacional de Ensino e Pesquisa (RNP), e o Centro de Estudos, Resposta e Tratamentos de Incidentes de Segurança no Brasil (Cert.br), que faz a gestão de incidentes para redes do Comitê Gestor da Internet no Brasil (CGI.br). Essas entidades se articulam com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov).

Para Calil, a Anatel ajuda a equilibrar esse jogo de forças, ampliando a participação social. Em 2021, a agência criou o Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestrutura Crítica (GT-Ciber), reunindo empresas de telecomunicações. O grupo editou o Ato 77, da Anatel, de julho de 2021, que estabelece requisitos de segurança cibernética para aparelhos de telecomunicações e dispositivos conectados à internet, como roteadores, modems, celulares, câmeras de segurança e televisões.

"Agora, aguardamos a interação com o novo governo e uma participação mais intensa na atualização da estratégia nacional", afirma Gustavo Santana Borges, superintendente de controle de obrigações da agência e integrante do GT-Ciber. ■

Os artigos científicos consultados para esta reportagem estão listados na versão on-line.

INFOGRÁFICO ALEXANDRE AFFONSO / REVISTA PESQUISA FAPESP