CÂMARA DOS DEPUTADOS

COMISSÃO DE CIÊNCIA, TECNOLOGIA E INOVAÇÃO

PROJETO DE LEI Nº 1.971, DE 2023

Altera a Lei nº 12.965, de 23 de abril de 2014, para dispor sobre a segurança cibernética de aparelhos eletrônicos com acesso à internet comercializados no país.

Autor: Deputado ZÉ VITOR

Relator: Deputado DR. ZACHARIAS CALIL

I - RELATÓRIO

Trata o presente projeto de lei sobre a segurança cibernética de aparelhos eletrônicos com acesso à internet comercializados no Brasil.

A proposta determina que aparelhos eletrônicos com acesso à internet somente sejam comercializados no País caso contenham sistemas de segurança que os protejam contra instalação de programas maliciosos, invasão por terceiros e vazamento de dados pessoais.

As funcionalidades e requisitos mínimos dos referidos sistemas, a serem detalhados em regulamentação, incluirão a previsão de atualizações regulares para proteção a novos programas maliciosos, falhas de segurança e métodos de invasão.

As sanções a serem impostas na hipótese de descumprimento ao disposto na proposta sujeitam o infrator às penalidades previstas no Código de Defesa do Consumidor.

O projeto não possui apensos e foi distribuído às Comissões de Ciência, Tecnologia e Inovação; Defesa do Consumidor e Constituição e Justiça e de Cidadania (art. 54 RICD).

A apreciação da proposição é conclusiva pelas Comissões e seu regime de tramitação é o ordinário, conforme o art. 24, inciso II e art. 151, inciso III, ambos do Regimento Interno da Câmara dos Deputados (RICD).

É o relatório.

II - VOTO DO RELATOR

O crescimento no uso de dispositivos móveis no Brasil e no mundo tem sido acompanhado por um aumento significativo nas fraudes online.

Segundo um relatório da NortonLifeLock, em 2022, nos Estados Unidos, 59% dos usuários de smartphones norte-americanos foram alvo de cibercrimes, de alguma forma de fraude ou ataque cibernético[1]. Estes ataques variam desde *phishing* e *malware* até roubo de identidade, refletindo a necessidade urgente de reforçar a segurança digital nos dispositivos móveis. No Brasil, o número salta para 69%, conforme o mesmo relatório.

Segundo a Federação Brasileira de Bancos (Febraban), houve um aumento de 80% nas tentativas de fraude via aplicativos bancários e internet banking em 2021, comparado ao ano anterior em nosso país. Este crescimento destaca a vulnerabilidade dos dispositivos móveis e a necessidade de medidas de segurança mais rigorosas.

Ataques de *phishing*, por exemplo, são extremamente comuns. Muitas dessas tentativas são feitas via mensagens de texto (SMS) ou aplicativos de mensagens instantâneas, explorando a confiança dos usuários em comunicações aparentemente legítimas. Esse tipo de fraude pode levar ao comprometimento de informações pessoais e financeiras, causando prejuízos significativos aos usuários.

E esses ataques de *phishing* são especialmente prevalentes no Brasil. De acordo com o relatório da Kaspersky[2], o país lidera o ranking mundial de ataques de phishing, com mais de 20% dos usuários de internet tendo sido alvo de tentativas desse ilícito em 2022. Os ataques geralmente ocorrem

[1] Ver em: **2022 Cyber Safety Insights Report,** Global Results. Disponível em: https://www.nortonlifelock.com/us/en/newsroom/press-kits/2022-norton-cyber-safety-insights-report-special-release-online-creeping/ . Acesso em 28/05/2024.

[2] Ver em: https://www.kaspersky.com.br/blog/panorama-ameacas-latam-2022/20311/ Acesso em 28/05/2024.

através de mensagens de texto (SMS) ou aplicativos de mensagens instantâneas, onde os fraudadores se passam por instituições financeiras ou outros serviços confiáveis para roubar informações pessoais e financeiras.

Além disso, o Brasil também enfrenta um alto número de ataques de *malware* em dispositivos móveis. Segundo a PSafe, empresa de segurança digital, foram realizados mais de 2,6 milhões de bloqueios em tentativas de ataques apenas *malware* Trojan, entre janeiro e março de 2022[3]. Esses *malwares* podem roubar dados pessoais, monitorar atividades online e até mesmo controlar remotamente os dispositivos infectados, representando um risco significativo para a segurança dos usuários.

O uso de redes Wi-Fi públicas constitui outra área de preocupação. São redes, muitas vezes inseguras, alvos frequentes de hackers que podem interceptar dados transmitidos, incluindo senhas e informações de login. A falta de segurança das redes Wi-Fi públicas facilita ataques em que a comunicação entre o usuário e o provedor de aplicações é interceptada sem que o usuário perceba.

Também o roubo de identidade é um problema crescente no Brasil. Estudo da Experian mostra que 61% dos brasileiros já passaram por alguma experiência deste tipo ou conhecem alguém que foi vítima[4]. Só em 2022 houve um aumento de 21,7% nos casos de roubo de identidade, com muitos deles originados de fraudes online cometidas por meio de dispositivos móveis. Os criminosos utilizam informações pessoais roubadas para abrir contas, realizar compras fraudulentas e cometer outros crimes, causando grandes prejuízos às vítimas.

As muitas estatísticas ruins sublinham a importância de adotar medidas de segurança robustas nos dispositivos móveis no Brasil, como o uso de autenticação de dois fatores, softwares de segurança e a conscientização sobre os perigos das redes Wi-Fi públicas e mensagens de phishing. É essencial que os usuários brasileiros estejam bem informados e vigilantes para

[3] Ver em: https://www.cisoadvisor.com.br/trojan-e-o-malware-que-predomina-nos-ataques-de-2022/ Acesso em 24/05/2024.

[4] Ver segundo o Relatório Global de Identidade e Fraude 2022 da Experian. Ver em: https://www.serasaexperian.com.br/images-cms/wp-content/uploads/2022/09/Relatorio-Global-de-Identidade-e-Fraude_Outubro2022.pdf Acesso em 28/05/2024.

se protegerem contra as crescentes ameaças cibernéticas que acompanham o uso intensivo de smartphones. Tudo isso é importante, porém não suficiente.

Da mesma forma, é relevante que os próprios aparelhos eletrônicos com acesso à internet contenham sistemas de segurança aptos a proteger contra a instalação de programas maliciosos, invasão por terceiros e os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Embora a proposta legislativa seja meritória, entendemos que alguns ajustes deveriam ser promovidos. No novo art. 29-A sugerimos que, ao invés da expressão “vazamentos de dados”, seja empregada locução semelhante àquela utilizada pela Lei Geral de Proteção de Dados Pessoais – LGPD, que aduz a necessária utilização de medidas técnicas aptas a proteger dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Do mesmo modo, entendemos que a determinação do que seja razoável a levar em consideração na utilização das referidas medidas técnicas deve envolver fatores objetivos, tais como custo e tempo necessários para evitar as ações ilícitas, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

Dessa forma, na certeza de que a presente iniciativa contribuirá para promover a segurança e tranquilidade aos cidadãos, pedimos o apoio dos nobres Deputados para a APROVAÇÃO do presente Projeto de Lei, na forma do SUBSTITUTIVO em anexo.

Sala da Comissão, em 03 de junho de 2024.

Deputado DR. ZACHARIAS CALIL

Relator

COMISSÃO DE CIÊNCIA, TECNOLOGIA E INOVAÇÃO

SUBSTITUTIVO AO PROJETO DE LEI Nº 1.971, DE 2023

Altera a Lei nº 12.965, de 23 de abril de 2014, para dispor sobre a segurança cibernética de aparelhos eletrônicos com acesso à internet comercializados no país.

O Congresso Nacional decreta:

Art. 1º A Lei nº 12.965, de 23 de abril de 2014, passa a vigorar acrescida do seguinte art. 29-A:

"Art. 29-A. Os aparelhos eletrônicos que permitam acesso à internet só poderão ser comercializados no País se contiverem sistemas de segurança que garantam medidas técnicas e aptas razoáveis a proteger contra a instalação de programas maliciosos, a invasão por terceiros e os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para evitar as ações ilícitas descritas no caput, de acordo com as tecnologias disponíveis.

§ 2° A regulamentação disporá sobre as funcionalidades e requisitos mínimos dos sistemas previstos no caput, que incluirão a previsão de atualizações regulares para proteção a novos programas maliciosos, falhas de segurança e métodos de invasão.

§ 3° O descumprimento ao disposto neste artigo ou à regulamentação prevista no parágrafo anterior sujeita o infrator

às sanções previstas na Lei nº 8.078, de 11 de setembro de 1990 – Código de Defesa do Consumidor, e demais normas de defesa do consumidor."

Art. 2º Esta lei entra em vigor 90 (noventa) dias após a data de sua publicação.

Sala da Comissão, em 03 de junho de 2024.

Deputado DR. ZACHARIAS CALIL
Relator