Apresentação: 29/10/2025 17:54:34.423 - CCTI
PRL 2 CCTI => PL 1971/2023
PRL n.2

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).

CD255632853700

Para verificar a assinatura, acesse https://infoleg-autenticidade-assinatura.camara.leg.br/CD255632853700
Assinado eletronicamente pelo(a) Dep. Dr. Zacharias Calil

Apresentação: 29/10/2025 17:54:34.423 - CCTI
PRL 2 CCTI => PL 1971/2023
PRL n.2

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).

Em 03 de junho de 2024, apresentei parecer pela aprovação, com substitutivo. Findo o prazo regimental, não foram apresentadas emendas ao substitutivo. Entretanto, após receber manifestações oficiais de Anatel, Senacon/MJSP, ANPD e MCTI, bem como os documentos públicos da indústria (ABINEE) e de entidades de defesa do consumidor, optou-se por elaborar um novo substitutivo, no sentido de calibrar obrigações, segundo o risco dos dispositivos.

Os elementos colhidos revelaram a conveniência de:

1. classificar dispositivos em níveis de criticidade, afinando as exigências;

2. estabelecer prazos de atualização proporcionais à criticidade;

3. reconhecer certificações internacionais para evitar duplicidade de custos;

4. criar governança permanente e apoio a micro e pequenas empresas; e

5. escalonar a entrada em vigor da norma.

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

CD255632853700

Para verificar a assinatura, acesse https://infoleg-autenticidade-assinatura.camara.leg.br/CD255632853700
Assinado eletronicamente pelo(a) Dep. Dr. Zacharias Calil

Apresentação: 29/10/2025 17:54:34.423 - CCTI
PRL 2 CCTI => PL 1971/2023
PRL n.2

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 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

---

[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.

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

Para verificar a assinatura, acesse https://infoleg-autenticidade-assinatura.camara.leg.br/CD255632853700
Assinado eletronicamente pelo(a) Dep. Dr. Zacharias Calil

CD255632853700

Apresentação: 29/10/2025 17:54:34.423 - CCTI
PRL 2 CCTI => PL 1971/2023
PRL n.2

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 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.

[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.

CD255632853700

Para verificar a assinatura, acesse https://infoleg-autenticidade-assinatura.camara.leg.br/CD255632853700
Assinado eletronicamente pelo(a) Dep. Dr. Zacharias Calil

Apresentação: 29/10/2025 17:54:34.423 - CCTI
PRL 2 CCTI => PL 1971/2023
PRL n.2

Embora a proposta legislativa seja meritória, entendemos que alguns ajustes deveriam ser promovidos. O substitutivo ora apresentado prevê as seguintes alterações:

1. classifica os dispositivos em três níveis de risco (alto, médio e baixo), permitindo que apenas os de maior criticidade demandem certificação de terceira parte;

2. estabelece prazos de atualização proporcionais (24, 18 e 12 meses), reduzindo o ônus de suporte em produtos de menor impacto;

3. admite autodeclaração auditável para níveis médios e baixos, com auditoria por amostragem bienal;

4. reconhece selos internacionais equivalentes, evitando dupla certificação e encarecimento indevido;

5. institui Comitê Técnico Tripartite, garantindo revisão bienal de requisitos em conjunto com Anatel, Senacon/MJSP, ANPD, MCTI, indústria e defesa do consumidor;

6. cria Fundo de Apoio às MPE, financiado por até 10 % das multas aplicadas, sem gerar despesa obrigatória direta; e

7. define *vacatio legis* progressiva de 180 dias para dispositivos inéditos e 360 dias para modelos existentes, permitindo adaptação gradual e escoamento de estoques.

A análise das posições oficiais dos órgãos competentes (Anatel, Senacon/MJSP, ANPD e MCTI), bem como dos documentos públicos da indústria (ABINEE) e de entidades de defesa do consumidor, fundamenta-se em evidências técnicas que indicam a eficácia de modelos escalonados de compliance em cibersegurança, sem transferir custos desproporcionais ao consumidor final. Considera-se, portanto, que o substitutivo apresentado resguarda a segurança da informação, alinhado a padrões internacionais; minimiza impacto inflacionário e barreiras de mercado, sobretudo para micro e pequenas empresas e fortalece o regime de proteção ao consumidor.

CD255632853700

Para verificar a assinatura, acesse https://infoleg-autenticidade-assinatura.camara.leg.br/CD255632853700
Assinado eletronicamente pelo(a) Dep. Dr. Zacharias Calil

Apresentação: 29/10/2025 17:54:34.423 - CCTI
PRL 2 CCTI => PL 1971/2023
PRL n.2

Pelas razões expostas, na certeza do mérito e oportunidade da proposição, meu voto é pela APROVAÇÃO do Projeto de Lei nº 1.971, de 2023, na forma do Substitutivo anexo.

Sala da Comissão, em de de 2025.

Deputado DR. ZACHARIAS CALIL
Relator

2025-16823

CD255632853700

Para verificar a assinatura, acesse https://infoleg-autenticidade-assinatura.camara.leg.br/CD255632853700
Assinado eletronicamente pelo(a) Dep. Dr. Zacharias Calil

Apresentação: 29/10/2025 17:54:34.423 - CCTI
PRL 2 CCTI => PL 1971/2023
PRL n.2

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 requisitos mínimos de segurança cibernética de dispositivos eletrônicos com acesso à internet e dá outras providências.

O Congresso Nacional decreta:

Art. 1º Esta Lei altera a Lei nº 12.965, de 23 de abril de 2014, para dispor sobre requisitos mínimos de segurança cibernética de dispositivos eletrônicos com acesso à internet e dá outras providências.

Art. 2º Incluam-se os arts. 29-A, 29-B e 29-C na Lei nº 12.965, de 23 de abril de 2014, com a seguinte redação:

.....

"Art. 29-A. A fabricação, a importação e a comercialização, no País, de dispositivo eletrônico dotado de capacidade de conexão à internet atenderá, no mínimo, os seguintes requisitos:

I – classificação, conforme o grau de risco para a segurança da informação e a integridade das redes, nos seguintes níveis, na forma do regulamento:

a) Nível I — alto risco;

b) Nível II — médio risco; e

c) Nível III — baixo risco.

II - para cada nível de risco, o regulamento definirá, no mínimo, mecanismos de prevenção à instalação de programas maliciosos, de proteção contra acesso não autorizado ou invasão por terceiros e de mitigação de vazamento de dados pessoais.

CD255632853700

Para verificar a assinatura, acesse https://infoleg-autenticidade-assinatura.camara.leg.br/CD255632853700
Assinado eletronicamente pelo(a) Dep. Dr. Zacharias Calil

Apresentação: 29/10/2025 17:54:34.423 - CCTI
PRL 2 CCTI => PL 1971/2023
PRL n.2

IIII – disponibilização de atualizações de segurança no prazo mínimo de:

a) 24 (vinte e quatro) meses, para dispositivos de Nível I;

b) 18 (dezoito) meses, para dispositivos de Nível II;

c) 12 (doze) meses, para dispositivos de Nível III.

§ 1º Para dispositivos dos Níveis II e III, o atendimento aos requisitos de que trata este artigo poderá ser comprovado por declaração do fabricante ou importador, sujeita a auditoria por amostragem bienal, nos termos do regulamento.

§ 2º Serão considerados equivalentes, para fins de comprovação de conformidade, os selos ou certificações internacionais listadas pelo Comitê de que trata o art. 29-B.

§ 3º O descumprimento do disposto neste artigo ou no regulamento sujeita o infrator às sanções previstas na Lei nº 8.078, de 11 de setembro de 1990, sem prejuízo de outras sanções administrativas, civis ou penais cabíveis.

§ 4º Aplica-se este artigo no prazo de 180 (cento e oitenta) dias, no caso de dispositivos eletrônicos inéditos, e de 360 (trezentos e sessenta) dias, no caso de dispositivos já homologados ou em produção até a data da publicação desta Lei.

Art. 29-B. Fica instituído o Comitê Técnico Tripartite de Segurança de Dispositivos Conectados, com a finalidade de:

I – propor e revisar, bienalmente, os requisitos mínimos de segurança cibernética referidos no art. 29-A;

II – elaborar e atualizar a lista de certificações ou selos de conformidade reconhecidos para os fins de cumprimento no previsto no § 2º do art. 29-A; e

III – acompanhar a evolução tecnológica e recomendar ajustes ao regulamento.

CD255632853700

Para verificar a assinatura, acesse https://infoleg-autenticidade-assinatura.camara.leg.br/CD255632853700
Assinado eletronicamente pelo(a) Dep. Dr. Zacharias Calil

Apresentação: 29/10/2025 17:54:34.423 - CCTI
PRL 2 CCTI => PL 1971/2023
PRL n.2

§ 1º O comitê de que trata este artigo será composto por, no mínimo, representantes:

I – do Ministério da Ciência, Tecnologia e Inovação;

II – da Secretaria Nacional do Consumidor Ministério da Justiça e Segurança Pública;

III – da Agência Nacional de Telecomunicações – Anatel;

IV – da Autoridade Nacional de Proteção de Dados – ANPD;

V – de entidades representativas da indústria de dispositivos conectados;

VI – de organizações da sociedade civil de defesa do consumidor.

§ 2º A participação no Comitê é considerada prestação de serviço público relevante, não remunerada.

§ 3º O regulamento disporá sobre a organização e o funcionamento do Comitê.”

“Art. 29-C. Fica instituído o Fundo de Apoio à Adequação de Micro e Pequenas Empresas à Segurança Cibernética de Dispositivos Conectados, destinado a financiar projetos de microempresas e empresas de pequeno porte voltados ao desenvolvimento ou à adaptação de firmware e hardware para atendimento aos requisitos desta Lei.

§ 1º O Fundo será constituído por até 10 % (dez por cento) do produto das multas aplicadas com fundamento no art. 29-A.

§ 2º Ato do Poder Executivo disporá sobre a gestão, a aplicação dos recursos e os critérios de seleção dos projetos.

.....”

Art. 3º Esta Lei entra em vigor na data de sua publicação.

CD255632853700

Para verificar a assinatura, acesse https://infoleg-autenticidade-assinatura.camara.leg.br/CD255632853700
Assinado eletronicamente pelo(a) Dep. Dr. Zacharias Calil

Apresentação: 29/10/2025 17:54:34.423 - CCTI
PRL 2 CCTI => PL 1971/2023
PRL n.2

Sala da Comissão, em de de 2025.

Deputado DR. ZACHARIAS CALIL
Relator

2025-16823

CD255632853700

Para verificar a assinatura, acesse https://infoleg-autenticidade-assinatura.camara.leg.br/CD255632853700
Assinado eletronicamente pelo(a) Dep. Dr. Zacharias Calil