CÂMARA DOS DEPUTADOS

PROJETO DE LEI N.º 428, DE 2024

(Do Sr. Carlos Zarattini)

Altera a Lei nº 12.965, de 23 de abril de 2014 – Marco Civil da Internet, para dispor sobre a segurança cibernética na prestação de serviços e atividades econômicas que empreguem sistemas de informação em sua prestação, e a comunicação aos órgãos reguladores e fiscalizadores incidente de cibersegurança material e ameaças de cibersegurança.

DESPACHO:
ÀS COMISSÕES DE
INDÚSTRIA, COMÉRCIO E SERVIÇOS;
COMUNICAÇÃO E
CONSTITUIÇÃO E JUSTIÇA E DE CIDADANIA (ART. 54 RICD)

APRECIAÇÃO:
Proposição Sujeita à Apreciação Conclusiva pelas Comissões - Art. 24 II

PUBLICAÇÃO INICIAL
Art. 137, caput - RICD

PROJETO DE LEI Nº , DE 2024
(Do Sr. CARLOS ZARATTINI)

Altera a Lei nº 12.965, de 23 de abril de 2014 – Marco Civil da Internet, para dispor sobre a segurança cibernética na prestação de serviços e atividades econômicas que empreguem sistemas de informação em sua prestação, e a comunicação aos órgãos reguladores e fiscalizadores incidente de cibersegurança material e ameaças de cibersegurança.

O Congresso Nacional decreta:

Art. 1º Esta Lei altera a Lei nº 12.965, de 23 de abril de 2014 – Marco Civil da Internet, para dispor sobre a segurança cibernética na prestação de serviços e atividades econômicas que empreguem sistemas de informação em sua prestação, e a comunicação aos órgãos reguladores e fiscalizadores incidente de cibersegurança material e ameaças de cibersegurança.

Art. 2° A Lei nº 12.965, de 2014, passa a vigorar com as seguintes alterações:

"Art. 5º Para os efeitos desta Lei, considera-se:

.....

IX – agente de mercado: a empresa, cooperativa ou entidade de direito privado que preste serviços ao público em geral, e que faça uso de sistemas de informação, para qualquer finalidade.

X - Incidente de cibersegurança: uma ocorrência não autorizada, ou uma série de ocorrências não autorizadas relacionadas com, em, ou conduzidas através dos sistemas de informação de um agente de mercado que comprometem a confidencialidade, integridade ou disponibilidade dos respectivos sistemas de informação ou de qualquer informação neles contida.

XI - Ameaça de cibersegurança: qualquer ocorrência potencial não autorizada em, ou conduzida através de sistemas de informação de

um agente de mercado que possa resultar em efeitos adversos sobre a confidencialidade, integridade ou disponibilidade dos respectivos sistemas de informação ou de qualquer informação neles contida.

XII - Sistemas de informação: recursos de informação eletrônicos, de propriedade ou usados pelo agente de mercado, incluindo infraestrutura física ou virtual controlada por tais recursos de informação, ou componentes deles, organizados para a coleta, processamento, manutenção, uso, compartilhamento, disseminação ou disposição das informações do agente de mercado para manter ou apoiar as respectivas operações.

XIII - Gerenciamento de riscos e estratégia: documento que descreve os processos do agente de mercado para avaliar, identificar e gerenciar riscos materiais provenientes de ameaças de cibersegurança com detalhes suficientes para que um usuário médio compreenda esses processos, e os riscos provenientes de ameaças de cibersegurança, incluindo como resultado de incidentes de cibersegurança anteriores, afetaram materialmente ou têm probabilidade razoável de afetar materialmente o agente de mercado, incluindo sua estratégia de negócios, resultados operacionais ou condição financeira.

XII – Governança: o sistema interno por meio do qual é efetivada a supervisão por órgãos de gestão do agente de mercado em relação aos riscos provenientes de ameaças de cibersegurança, incluindo conselhos de administração, comitê ou subcomitê do conselho responsável pela supervisão dos riscos provenientes de ameaças de cibersegurança, e os processos pelos quais o conselho ou tal comitê é informado sobre tais riscos.” (NR)

“CAPITULO III-A

Das medidas de Cibersegurança

Art. 23-A Os agentes de mercado submeterão ao respectivo órgão regulador e fiscalizador informe sobre o papel dos respectivos sistemas de governança na avaliação e gestão dos riscos materiais provenientes de ameaças de cibersegurança, abordando, conforme aplicável, os seguintes aspectos, sem prejuízo de outros estabelecidos em regulamento:

I - Se e quais posições ou comitês de gestão são responsáveis pela avaliação e gestão de tais riscos, e a expertise relevante dessas pessoas ou membros em detalhes suficientes para descrever totalmente a natureza da expertise;

II - Os processos pelos quais essas pessoas ou comitês são informados e monitoram a prevenção, detecção, mitigação e remediação de incidentes de cibersegurança; e

III- Se essas pessoas ou comitês reportam informações sobre tais riscos ao conselho ou comitês.

IV – As qualificações técnicas dos gestores responsáveis pelo gerenciamento de riscos em cibersegurança, incluindo a experiência de trabalho anterior em cibersegurança; quaisquer diplomas ou certificações relevantes; qualquer conhecimento, habilidades ou outra formação em cibersegurança.” (NR)

“Art. 23-B Os agentes de mercado informarão, no prazo de até cinco dias úteis a partir da ocorrência do evento, por meio de sistema eletrônico a ser instituído pelo respectivo órgão regulador e fiscalizador, a menos que lei específica disponha em sentido diverso, nos termos estabelecidos em regulamento, a ocorrência de:

I - incidente de cibersegurança material;

II - ameaça de cibersegurança.

§ 1º As informações de que trata o “caput” incluirão, pelo menos, no caso de incidente de cibersegurança que seja determinado pelo agente de mercado como significativo, observados os critérios estabelecidos pelo órgão regulador e fiscalizador, informação sobre a natureza, alcance e cronologia do incidente, e o impacto significativo ou razoavelmente provável no agente de mercado, incluindo sua condição financeira e resultados das operações, e avaliação dos riscos para direitos de usuários e consumidores decorrentes da ocorrência e as providências para a sua correção ou compensação.

§ 2º. No caso de agente de mercado que opere no mercado de valores mobiliários, títulos de crédito, serviços bancários ou financeiros, inclusive cartões de crédito ou débito, seguros, seguro saúde e previdência privada, deverá informar as medidas de

auditoria já realizadas ou em fase de realização, visando ao restabelecimento níveis de segurança necessários à proteção de ativos de seus clientes, usuários ou correntistas.

§ 3º Caberá ao órgão regulador e fiscalizador avaliar a conveniência e oportunidade da divulgação ao público dos incidentes ou ameaças de que trata o "caput", considerada a ocorrência de risco substancial para a segurança nacional ou a segurança pública, o direito à privacidade de dados e os impactos econômicos no setor regulado.

§ 4º O órgão regulador e fiscalizador apurará a responsabilidade do agente de mercado em relação a um incidente de cibersegurança, e aplicará as sanções cabíveis, assegurada a ampla defesa."(NR)

"Art. 23-C. As microempresas e empresas de pequeno porte sujeitas ao disposto nesta Lei disporão de prazos em dobro para a adoção das medidas de cibersegurança de que tratam os art. 23-A e 23-B desta Lei."(NR)

Art. 3º. Esta Lei entra em vigor 60 (sessenta) dias a partir da data da sua publicação.

JUSTIFICAÇÃO

Em 26 de dezembro de 2023, o Presidente da República Luiz Inácio Lula da Silva editou o Decreto 11.856, que "Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança".

Entre os objetivos desta Política, estão os de garantir a confidencialidade, a integridade, a autenticidade e a disponibilidade das soluções e dos dados utilizados para o processamento, o armazenamento e a transmissão eletrônica ou digital de informações, fortalecer a atuação diligente no ciberespaço, especialmente das crianças, dos adolescentes e dos idosos, contribuir para o combate aos crimes cibernéticos e às demais ações maliciosas no ciberespaço e estimular a adoção de medidas de proteção cibernética e de gestão de riscos para prevenir, evitar, mitigar, diminuir e neutralizar

vulnerabilidades, incidentes e ataques cibernéticos, e seus impactos. Além disso, objetiva incrementar a resiliência das organizações públicas e privadas a incidentes e ataques cibernéticos, desenvolver a educação e a capacitação técnico-profissional em segurança cibernética na sociedade, incrementar a atuação coordenada e o intercâmbio de informações de segurança cibernética entre os níveis de Governo e Poderes, setor privado e sociedade, e desenvolver mecanismos de regulação, fiscalização e controle destinados a aprimorar a segurança e a resiliência cibernéticas nacionais.

A preocupação apontada pelo Chefe do Executivo é não somente oportuna, mas essencial à proteção da sociedade contra os crimes cibernéticos, que a Lei nº 12.737, de 30 de novembro de 2012, definiu ao promover alterações ao Código Penal. Entre eles, temos os crimes de Invasão de dispositivo informático (art. 154-A), e o de Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública" (art. 266).

A preocupação com as ameaças e incidentes de cibersegurança é um tema global, e a necessidade de que sejam adotadas medidas para garantir a segurança dos sistemas de informação vem merecendo a atenção dos governos e adoção de novas leis e medidas regulatórias que ampliem a responsabilização dos agentes de mercado diante de clientes, consumidores, usuários de serviços e partes relacionadas.

A cada incidente, milhões de cidadãos e empresas sofrem prejuízos, algumas vezes irreversíveis.

Segundo a IBM, o custo médio global de uma violação de dados em 2023 foi de US$ 4,45 milhões, e 51% organizações planejavam aumentar os investimentos em segurança por conta de uma violação que sofreram, incluindo planejamento e teste de resposta a incidentes (RI), treinamento de funcionários e ferramentas de detecção e resposta a ameaças. A FEBRABANTECH informa que o Brasil é o país latino-americano que mais sofre com ataques cibernéticos: apenas no 1º semestre de 2023, foram 23 bilhões de tentativas de ataques.

Nos EUA, em agosto de 2023 a Securities and Exchange Commission – SEC, entidade que regula o sistema de valores mobiliários e câmbio, adotou novas regras para aprimorar e padronizar as divulgações relacionadas à gestão de riscos cibernéticos, estratégia, governança e incidentes por parte de empresas de capital aberto sujeitas aos requisitos de relatórios da Lei de Bolsas de Valores de 1934.

As novas regras, que foram, após consulta pública, incorporadas ao "Code of Federal Regulations", que consolida as normas regulatórias, inclui a obrigação de as empresas divulgarem incidentes cibernéticos materiais, e de promoverem divulgações periódicas sobre os processos adotados para avaliar, identificar e gerenciar riscos cibernéticos materiais, e sobre o papel da administração na avaliação e gestão de riscos cibernéticos materiais. A norma entrou em vigor em 5 de setembro de 2023.

No Brasil, apesar do disposto no Decreto editado, e de algumas previsões legais, como o disposto no art. 38 da Lei Geral de Proteção de Dados, que prevê que a ANPD "poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial", não há normas legais que estabeleçam obrigações da mesma natureza, quer para as empresas que tenham ações negociadas em bolsa, quer para empresas de capital fechado, ou quaisquer outras pessoas jurídicas que estejam expostas a ameaças ou incidentes de cibersegurança e, com isso, vulneráveis à exposição de dados de seus clientes ou usuários ou de suas operações e ativos.

No âmbito do Governo Federal, o Centro Integrado de Segurança Cibernética do Governo Digital (CISC Gov.br) proporciona aos órgãos do SISP suporte para promover efetividade na prevenção, tratamento e resposta a incidentes, e pode atuar em caso de incidentes notificados, para prestar orientações técnicas quanto às boas práticas de tratamento e resposta a incidentes e alocando de forma pontual e temporária equipe especializada para rápido tratamento e resposta ao incidente. O CISC Gov.br tem o compromisso de manter seu público informado sobre as tendências de ameaças cibernéticas, e eventuais notificações de incidente recebidas por parceiros serão tratadas e compartilhadas com órgãos afetados.

O Conselho Nacional de Justiça, por meio da Resolução nº 396/2021, instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), que é um conjunto de requisitos e de boas práticas, com o objetivo de estabelecer diretrizes e requisitos para aumentar a segurança do ambiente tecnológico dos órgãos do Poder Judiciário. Também em 2021 foi publicada, pelo CNJ, a Portaria nº 162/2021, que aprova protocolos e manuais criados pela ENSEC-PJ, dispondo sobre o Protocolo de Prevenção a Incidentes Cibernéticos (PPINC-PJ), que tem por objetivo principal o estabelecimento de um conjunto de diretrizes para a prevenção de incidentes cibernéticos; o

Protocolo de Gerenciamento de Crises Cibernéticas (PGCRC-PJ), que tem por objetivo principal estabelecer um conjunto de diretrizes para responder efetivamente a crises decorrentes de incidentes cibernéticos; e o Protocolo de Investigação de Ilícitos Cibernéticos (PIILC-PJ) que tem por objetivo principal estabelecer os procedimentos básicos para coleta e preservação de evidências e para comunicação obrigatória dos fatos penalmente relevantes ao Ministério Público e ao órgão de polícia judiciária com atribuição para o início da persecução penal.

O presente projeto de lei, assim, visa, em consonância com a Política Nacional de Cibersegurança – PNCiber, introduzir na Lei do Marco Civil da Internet provisões para dispor, em caráter geral, sobre a segurança cibernética na prestação de serviços e atividades econômicas que empreguem sistemas de informação em sua prestação, e a comunicação aos órgãos reguladores e fiscalizadores incidente de cibersegurança material e ameaças de cibersegurança.

Além dos conceitos necessários à aplicação da norma, gerando obrigações legais a todos os agentes de mercado, definidos como “a empresa, cooperativa ou entidade de direito privado que preste serviços ao público em geral, e que faça uso de sistemas informação, para qualquer finalidade”, propomos que os agentes sejam obrigados a submeter ao respectivo órgão regulador e fiscalizador (que poderão ser agências reguladoras, ou a CVM, SUSEP ou Banco Central, conforme o caso) informe sobre o papel dos respectivos sistemas de governança na avaliação e gestão dos riscos materiais provenientes de ameaças de cibersegurança, abordando diversos aspectos das medidas adotadas para a avaliação e gestão de riscos, a qualificação de seu corpo técnico e sistemas de governança adotados, e as obrigação de que informem, por meio de sistema eletrônico a ser instituído pelo respectivo órgão regulador e fiscalizador, a ocorrência de incidente de cibersegurança material ou ameaça de cibersegurança. No caso de incidente de cibersegurança que seja determinado pelo agente de mercado como significativo, observados os critérios estabelecidos pelo órgão regulador e fiscalizador, deverão ser prestadas informações sobre a natureza, alcance e cronologia do incidente, e o impacto significativo ou razoavelmente provável no agente de mercado, incluindo sua condição financeira e resultados das operações, e avaliação dos riscos para direitos de usuários e consumidores decorrentes da ocorrência e as providências para a sua correção ou compensação.

E, no caso de agente de mercado que opere no mercado de valores mobiliários, títulos de crédito, serviços bancários ou financeiros, inclusive cartões de crédito ou débito, seguros, seguro saúde e previdência privada, o agente deverá informar as medidas de auditoria já realizadas ou em fase de realização, visando ao restabelecimento níveis de segurança necessários à proteção de ativos de seus clientes, usuários ou correntistas.

Contudo, em respeito às características de cada setor, caberá ao órgão regulador e fiscalizador avaliar a conveniência e oportunidade da divulgação ao público dos incidentes ou ameaças, considerada a ocorrência de risco substancial para a segurança nacional ou a segurança pública, o direito à privacidade de dados e os impactos econômicos no setor regulado.

Por fim, caberá ao órgão regulador e fiscalizador apurar a responsabilidade do agente de mercado em relação a um incidente de cibersegurança, e aplicará as sanções cabíveis, assegurada a ampla defesa.

Essas medidas, complementando o já disposto no Marco Civil da Internet e na Lei Geral de Proteção de Dados, e que no curso dos debates serão enriquecidas pelas contribuições dos Ilustres Pares, assim como do próprio Executivo a da sociedade, visam trazer ao debate a necessidade de uma proteção mais firme e sólida da segurança cibernética, com amparo legal, e que ultrapasse a lógica de “chorar sobre o leite derramado”.

A sociedade e o Poder Público têm o direito de não apenas ter imediata ciência de ameaças e incidentes, mas de exigir medidas preventivas e corretivas, que confiram a necessária confiança nos sistemas eletrônicos de dados e na proteção dos usuários, clientes e partes relacionadas.

Essa é a nossa intenção, ao apresentar a presente proposta, que esperamos poder contar com a aprovação dos Ilustres Pares.

Sala das Sessões,

DEPUTADO CARLOS ZARATTINI
PT/SP

LEI Nº 12.965, DE 23 DE ABRIL DE 2014	https://normas.leg.br/?urn=urn:lex:br:federal:lei:201404-23;12965

FIM DO DOCUMENTO