PROJETO DE LEI Nº , DE 2025

(Do Sr. JONAS DONIZETTE)

Altera a Lei nº 13.709, de 14 de agosto de 2018, para estabelecer regras adicionais acerca da comunicação de incidentes de segurança.

O Congresso Nacional decreta:

Art. 1º O art. 48 da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais) passa a vigorar com a seguinte redação:

"Art. 48. .....

.....

§ 1º A comunicação será feita no prazo de 10 (dez) dias úteis conforme definido pela autoridade nacional, contado do conhecimento pelo controlador de que o incidente afetou dados pessoais, e deverá mencionar, no mínimo:

.....

.....

§ 4º As informações poderão ser complementadas, de maneira fundamentada, no prazo de 40 (quarenta) dias úteis, a contar da data da comunicação.

§ 5º Os prazos constantes nos §§ 1º e 4º serão contados em triplo para microempresas e empresas de pequeno porte, bem como para iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação." **(NR)**

Art. 2º Esta lei entra em vigor na data da sua publicação.

JUSTIFICAÇÃO

A Lei Geral de Proteção de Dados Pessoais (LGPD), promulgada em 2018, representa um marco na legislação brasileira ao estabelecer normas claras para o tratamento de dados pessoais, promovendo maior segurança e privacidade em um mundo cada vez mais digital. Inspirada em legislações internacionais de vanguarda, como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, a LGPD é fundamental para garantir que tais informações dos cidadãos brasileiros sejam tratadas com responsabilidade e transparência. Sua adoção reflete o compromisso do Brasil com a proteção dos direitos dos titulares de dados e a adequação às melhores práticas globais.

Na sociedade contemporânea, na qual a economia digital se expande rapidamente e os dados pessoais se tornaram um recurso valioso, a proteção desses elementos não é apenas uma questão de privacidade, mas de dignidade humana. Informações pessoais, quando mal geridas ou expostas indevidamente, podem causar prejuízos financeiros, danos à reputação e até mesmo discriminação. Por isso, legislações como a LGPD se tornaram instrumentos indispensáveis para o equilíbrio entre o desenvolvimento tecnológico e a proteção dos direitos individuais, garantindo que os avanços digitais sejam acompanhados de segurança e respeito à privacidade.

Dentro desse contexto, a comunicação de incidentes de segurança emerge como um pilar crucial da legislação de proteção de dados. Quando ocorre um vazamento de informações ou qualquer outro incidente que coloque em risco os dados pessoais, é essencial que a organização responsável realize uma comunicação eficaz e precisa tanto com os titulares dos dados quanto com o órgão regulador competente. Esse diálogo permite que as pessoas afetadas tomem medidas preventivas para proteger seus direitos, como trocar senhas, monitorar suas contas financeiras ou buscar auxílio legal, se necessário. Além disso, a notificação ao órgão regulador possibilita uma resposta mais coordenada e adequada ao incidente. A transparência nesses momentos críticos fortalece a confiança entre as

empresas, os consumidores e as autoridades, além de minimizar os danos potenciais.

Contudo, para que essa comunicação seja verdadeiramente eficaz, ela deve ser, acima de tudo, confiável, dotada de ampla credibilidade e baseada em uma investigação prévia conclusiva. Informações incompletas ou errôneas podem não apenas gerar confusão e desconfiança entre os titulares, como também impedir que as medidas adequadas sejam tomadas para mitigar os danos. Nesse sentido, é imprescindível que as organizações tenham tempo suficiente para realizar uma investigação minuciosa e apurar com exatidão os detalhes do incidente antes de realizar qualquer notificação.

Em nossa análise, a regulamentação da LGPD atualmente vigente, nos moldes estabelecidos pela ANPD, está em contradição com este pressuposto da informação adequada e precisa. Embora seja inegável que a transparência nesse processo é vital, nos parece inquestionável que ela só pode ser efetivamente alcançada se houver, anteriormente, tempo hábil para que os entes promovam uma averiguação meticulosa, de modo a entender com precisão a natureza do incidente e a extensão de seus danos. Nesse sentido, os prazos estabelecidos pela Resolução CD/ANPD nº 15, de 24 de abril de 2024 impõem desafios significativos, ao exigir que o controlador comunique à ANPD e aos titulares o incidente em apenas três dias úteis. Esse prazo é insuficiente para lidar com a complexidade de muitos incidentes de segurança, especialmente em casos que envolvem ataques sofisticados, como por exemplo *ransomware* (um tipo de *malware* que bloqueia o acesso aos dados até que um resgate seja pago), *spear phishing* (um ataque direcionado em que o invasor se passa por uma pessoa confiável para obter informações sensíveis) ou exploração de vulnerabilidades *zero-day* (o uso de falhas de segurança desconhecidas pelos desenvolvedores para atacar sistemas antes que possam ser corrigidas).

Além disso, mesmo com a previsão de prazos dobrados para microempresas e agentes de pequeno porte contida na referida Resolução, o prazo de três dias úteis continua sendo limitante para essas organizações, que geralmente dispõem de menos recursos e equipes especializadas em segurança da informação. O resultado é que essas empresas, que são muitas

vezes as mais vulneráveis, têm menos capacidade de realizar investigações robustas dentro desse prazo, o que pode prejudicar a qualidade das informações repassadas aos titulares e à ANPD.

Em artigo publicado no jornal Valor Econômico, o advogado Felipe Palhares, especialista em proteção de dados e cibersegurança, tece críticas que vão ao encontro das nossas convicções. Palhares argumenta que a Resolução CD/ANPD nº 15, de 2024 impõe desafios significativos para as organizações, especialmente no que diz respeito aos prazos. Ele também ressalta que a transparência e a responsabilização são fundamentais, mas devem ser equilibradas com a realidade operacional das empresas, para que a legislação seja efetivamente aplicada sem causar prejuízos desnecessários ou comprometer a segurança cibernética das organizações[1].

Atentos a essa realidade, apresentamos o presente Projeto de Lei, que altera a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), para estabelecer novos prazos para a comunicação de incidentes de segurança. O projeto prevê que a comunicação de incidentes seja feita em até 10 dias úteis, contados do conhecimento pelo controlador de que o incidente afetou dados pessoais. As informações podem ser complementadas em até 40 dias úteis, a contar da data da comunicação inicial. Além disso, o projeto estabelece que os prazos sejam contados em triplo para microempresas, empresas de pequeno porte e startups ou empresas de inovação.

Acreditamos firmemente que a proposição que ora apresentamos a esta Casa trará impactos legislativos positivos ao abordar os principais desafios enfrentados pelas empresas no cumprimento dos prazos atuais de comunicação de incidentes de segurança. Em primeiro lugar, o aumento do prazo para 10 dias úteis permitirá que as empresas, especialmente em casos complexos, realizem investigações mais detalhadas e precisas, evitando que informações incompletas ou imprecisas sejam divulgadas apressadamente. Esse prazo mais amplo assegura uma compreensão mais adequada do incidente, o que beneficia tanto os controladores quanto os

[1] Palhares, Felipe. "Comunicação de incidentes de segurança da informação." *Valor Econômico*, 27 de maio de 2024. Disponível em: https://valor.globo.com/legislacao/coluna/comunicacao-de-incidentes-de-seguranca-da-informacao.ghtml. Acesso em: 23 de setembro de 2024.

titulares dos dados. Além disso, ao reduzir a pressão sobre as organizações, a proposta incentiva uma comunicação mais eficaz e completa, em vez de priorizar a rapidez à custa da qualidade da informação. Isso garante que os titulares recebam dados relevantes e corretos, o que lhes permitirá tomar medidas mais assertivas para proteger seus interesses e direitos.

Outro benefício é o prazo de 40 dias úteis para a complementação de informações, permitindo que as empresas apresentem dados fundamentados, baseados em uma investigação completa. Esse tempo adicional reduz a probabilidade de revisões contínuas e garante que o controlador forneça informações robustas e bem embasadas. Nossa proposição também proporciona maior previsibilidade e segurança jurídica para as empresas, já que os prazos mais longos asseguram um cumprimento adequado das exigências da LGPD sem a constante preocupação com penalidades resultantes de comunicações apressadas e potencialmente inadequadas.

Além disso, a proposta beneficia as microempresas, empresas de pequeno porte, startups e empresas inovadoras ao estabelecer prazos em triplo para essas entidades, reconhecendo suas limitações operacionais e a necessidade de mais tempo para gerenciar incidentes de segurança. Essa diferenciação é fundamental para garantir que essas empresas possam se adequar à legislação sem comprometer suas atividades principais. Ao proporcionar essas condições mais flexíveis, a proposta também serve como um incentivo adicional ao empreendedorismo e à inovação, criando um ambiente regulatório mais favorável ao desenvolvimento de novas tecnologias e negócios disruptivos.

A medida melhora ainda a capacidade das empresas de gerenciar crises de forma mais eficiente. O tempo adicional possibilita uma resposta mais bem estruturada e coordenada, que não apenas mitiga os danos causados pelos incidentes, mas também fortalece a confiança dos consumidores.

Outro impacto positivo será a redução de danos reputacionais. Com prazos mais adequados, as empresas terão tempo não apenas para

mitigar os efeitos do incidente, mas também para, ao comunicá-lo ao público, já informar as medidas concretas que foram postas em prática para sua contenção e resolução. Dessa forma, evita-se a divulgação prematura de informações incompletas, oferecendo ao público uma perspectiva mais completa e minimizando potenciais prejuízos à imagem da empresa.

Portanto, é com a plena convicção da conveniência e oportunidade do presente projeto de lei, e com a firme convicção de que ele contribuirá sobremaneira para assegurar que o tratamento de incidentes de segurança seja conduzido de maneira mais eficaz e responsável, que conclamamos o apoio dos nobres Parlamentares para sua aprovação.

Sala das Sessões, em de de 2025.

Deputado JONAS DONIZETTE

2024-9426