CÂMARA DOS DEPUTADOS

PROJETO DE LEI N.º 1.876-A, DE 2023

(Do Sr. Marcos Tavares)

Altera a Lei nº 13.709, de 14 de agosto de 2018, para obrigar a divulgação de incidentes de segurança de dados pessoais em veículos de comunicação social; tendo parecer da Comissão de Comunicação, pela aprovação deste e dos de nºs 272/24, 2138/24 e 3457/24, apensados, com Substitutivo (relator: DEP. JADYEL ALENCAR).

DESPACHO:
ÀS COMISSÕES DE:
COMUNICAÇÃO E
CONSTITUIÇÃO E JUSTIÇA E DE CIDADANIA (MÉRITO E ART. 54, RICD)

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

S U M Á R I O

PROJETO DE LEI Nº , de 2023.

(Do Sr. Marcos Tavares)

Altera a Lei nº 13.709, de 14 de agosto de 2018, para obrigar a divulgação de incidentes de segurança de dados pessoais em veículos de comunicação social.

O Congresso Nacional decreta:

Art. 1º Fica acrescido a Lei nº 13.709, de 14 de agosto de 2018, um artigo 54-A, com a seguinte redação:

"Art. 54-A Os agentes de tratamento deverão divulgar em veículos de comunicação social de grande circulação e em suas páginas e perfis, qualquer incidente de segurança que possa acarretar em risco ou dano relevante aos titulares, devendo informar o ocorrido à Autoridade Nacional de Proteção de Dados Pessoais." (NR)

Art. 2º O Poder Executivo estabelecerá as normas complementares necessárias à execução desta Lei.

Art. 3º Esta lei entra em vigor na data da sua publicação.

Sala das Sessões, em 13 de abril de 2023.

MARCOS TAVARES
Deputado Federal
PDT-RJ

JUSTIFICATIVA

Um dos problemas mais recorrentes com a sociedade da informação e da economia digital, é a quantidade de dados pessoais que circulam entre empresas e governos. Não é raro lermos notícias que relatam volumes descomunais de dados de titulares vazados, ou mesmo à venda, no mercado negro e outras plataformas.

Nesse cenário, o usuário não é informado sobre quando e quais dados foram objeto de incidente de segurança e, por isso, não é possível tomar as providências e precauções que naturalmente tomaria.

Sendo assim, entendemos ser acertado que os agentes de tratamento, ou seja, tanto controladores como operadores, nos termos da LGPD, sejam obrigados a divulgar em veículos de comunicação social de grande circulação, bem como em suas páginas e perfis dos provedores de aplicações, todo incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

Ademais, previmos, na presente iniciativa, que os agentes de tratamento devem informar o fato, tão logo ocorrido, para a Autoridade Nacional de Proteção de Dados Pessoais - ANPD.

Desse modo, é possível conceder maior transparência aos casos de vazamento de dados ou outros incidentes de segurança semelhantes, munindo o titular e a própria ANPD do conhecimento e dos meios para remediar os prejuízos deles decorrentes e até mesmo evita-los.

Diante do exposto e da importância fundamental do tema em questão, conclamamos os nobres pares desta Casa para aprovar o presente projeto de lei.

Sala das Sessões, em 13 de abril de 2023.

MARCOS TAVARES
Deputado Federal
PDT-RJ

LEGISLAÇÃO CITADA ANEXADA PELA
Coordenação de Organização da Informação Legislativa - CELEG
Serviço de Tratamento da Informação Legislativa - SETIL
Seção de Legislação Citada - SELEC

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018 **Art. 54-A**	https://normas.leg.br/?urn=urn:lex:br:federal:lei:201808-14;13709

PROJETO DE LEI N.º 272, DE 2024

(Do Sr. Júnior Mano)

Dispõe sobre prazo e medidas corretivas em caso de incidente de segurança no tratamento de dados pessoais pela Administração Pública, nos termos da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados (LGPD).

DESPACHO:
APENSE-SE À(AO) PL-1876/2023.

PROJETO DE LEI Nº , DE 2024

(Do Sr. JÚNIOR MANO)

Dispõe sobre prazo e medidas corretivas em caso de incidente de segurança no tratamento de dados pessoais pela Administração Pública, nos termos da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados (LGPD).

O Congresso Nacional decreta:

Art. 1º A Lei nº 13.709, de 14 de agosto de 2018, passa a vigorar acrescida do seguinte dispositivo:

"Art. 48-A Fica estabelecido o prazo de 05 (cinco) dias úteis, a contar da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, para que a Administração Pública, por meio do órgão ou entidade responsável pela irregularidade, no âmbito da União, Estados, Distrito Federal e Municípios, publique com destaque nas páginas de seus sítios oficiais um comunicado informando sobre o incidente.

§ 1º O comunicado descrito no caput permanecerá acessível ao público pelo prazo mínimo de 90 (noventa) dias.

§ 2º Sem prejuízo do disposto no § 1º, a Administração Pública, por meio da ANPD, enviará a todos os usuários do serviço mensagem de notificação, com informações sobre o incidente

de segurança e o endereço eletrônico do comunicado publicado no sítio oficial do órgão ou entidade responsável.

§ 3º Em caso de não cumprimento dos disposto neste artigo, caberá à ANPD a adoção e execução das medidas corretivas necessárias.” **(NR)**

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

JUSTIFICAÇÃO

Há um número crescente de incidentes de segurança, em especial de vazamento de dados pessoais, por parte de órgãos e entidades da Administração Pública. Podemos citar, por exemplo, o caso do Detran-RN, que vazou dados de quase 70 milhões de brasileiros[1], o caso do vazamento de dados referentes ao Auxílio Brasil, da Caixa Econômica e Dataprev, que afetou 4 milhões de pessoas[2], o caso do vazamento de dados pessoais vinculado a chaves PIX, o caso da operação *Deepwater*, que resultou na exposição dos dados pessoais de mais de 200 milhões de brasileiros, e assim por diante[3].

Em face desse problema, a crescente digitalização dos serviços governamentais e a massiva coleta e tratamento de dados pessoais pela Administração Pública tornam imperativa a criação de mecanismos eficazes para proteger a privacidade dos cidadãos. Assim, o presente projeto visa estabelecer prazos e medidas corretivas específicas em caso de incidentes de segurança, fortalecendo a transparência e a responsabilização dos órgãos e entidades públicos.

[1] Ver em: https://olhardigital.com.br/2019/10/08/noticias/exclusivo-detran-vaza-dados-pessoais-de-quase-70-milhoes-de-brasileiros/ Acesso em 15/02/2024.

[2] Ver em: https://www.convergenciadigital.com.br/Seguranca/Justica-condena-ANPD%2C-Caixa-e-Dataprev-por-vazamento-de-dados-do-Auxilio-Brasil-64291.html?UserActiveTemplate=mobile Acesso em 15/02/2024.

[3] Ver em: https://www.jota.info/tributos-e-empresas/mercado/vazamentos-de-dados-no-brasil-28012022 . Acesso em 15/02/2024.

A existência do Estado Social no desenvolvimento de políticas públicas e na distribuição de recursos pressupõe o tratamento de uma grande quantidade de dados, de modo a identificar e direcionar recursos, regular e fiscalizar atividades econômicas e mesmo investigar e promover a persecução penal.

O tratamento desse grande volume de dados pessoais pelo Estado, por sua vez, exige transparência e publicidade, tudo sem expor os dados pessoais dos cidadãos. Se de um lado há um risco de vigilância e abuso estatal, que são contrabalanceados pelos princípios constitucionais de impessoalidade e moralidade, por outro há um dever de eficiência e modernização do Estado, que deve utilizar os dados para a melhor prestação dos serviços.

Em casos de incidentes de segurança, o estabelecimento de um prazo para que haja resposta célere ao problema é muito importante, pois deixa os titulares cientes do problema e lhes dá a possibilidade de mudaram senhas de acesso e tomarem as precauções necessárias. Em face dos recentes e significativos vazamentos de dados por parte da Administração Pública, focamos nossos esforços no âmbito do poder público, incluindo órgãos e entidades pertencentes a União, Estados, Distrito Federal e Municípios.

Deve, então, o Poder Público mostrar que atende a finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, devendo informar o fundamento legal para o tratamento, indicar um encarregado e, não menos importante, dar publicidade às suas atividades de tratamento. Ademais, a Autoridade Nacional de Proteção de Dados Pessoais (ANPD) pode dispor sobre a forma dessa publicização.

Nessa toada, estabelecemos o prazo de 5 dias úteis, a contar da ocorrência do vazamento de dados pessoais, a fim de que a Administração Pública, por meio do órgão ou entidade responsável pelo incidente de segurança no âmbito da União, Estados, Distrito Federal e Municípios, publique com destaque nas páginas de seus sítios oficiais um comunicado informando sobre o incidente.

Determinamos, outrossim, que este comunicado permaneça acessível ao público pelo prazo mínimo de 90 dias, tempo a nosso ver necessário para que todo o público afetado tome conhecimento e possa agir para proteger efetivamente seus dados pessoais. Para fortalecer esse intento, determinamos que a Administração Pública, por meio da ANPD, encaminhe a todos os usuários do serviço objeto do incidente de segurança uma mensagem contendo informações sobre este incidente, e endereço eletrônico do comunicado publicado no sítio oficial do órgão ou entidade responsável.

Portanto, na certeza de que a presente iniciativa contribuirá para proteger o titular de dados na sua relação com a Administração Pública, pedimos o apoio dos nobres Deputados para a APROVAÇÃO do presente Projeto de Lei.

Sala das Sessões, em de de 2024.

Deputado JÚNIOR MANO

2024_521

CÂMARA DOS DEPUTADOS
CENTRO DE DOCUMENTAÇÃO E INFORMAÇÃO – CEDI
Coordenação de Organização da Informação Legislativa – CELEG

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018	https://normas.leg.br/?urn=urn:lex:br:federal:lei:201808-14;13709

PROJETO DE LEI N.º 2.138, DE 2024

(Do Sr. Ulisses Guimarães)

Altera a Lei nº 13.709, de 14 de agosto de 2018, para obrigar a divulgação em veículos de comunicação social e em provedores de aplicações a ocorrência de incidentes de segurança envolvendo dados pessoais e estabelecer critérios, prazos e penalidades para a sua efetivação.

DESPACHO:
APENSE-SE AO PL-1876/2023.

CÂMARA DOS DEPUTADOS
Deputado Federal Ulisses Guimarães MDB/MG

PROJETO DE LEI Nº , DE 2024

(Do Sr. Ulisses Guimarães)

Altera a Lei nº 13.709, de 14 de agosto de 2018, para obrigar a divulgação em veículos de comunicação social e em provedores de aplicações a ocorrência de incidentes de segurança envolvendo dados pessoais e estabelecer critérios, prazos e penalidades para a sua efetivação.

O Congresso Nacional decreta:

Art. 1º Esta lei altera a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), para incluir disposições sobre a comunicação de incidentes de segurança envolvendo dados pessoais, estabelecendo critérios, prazos e penalidades para assegurar a proteção dos direitos dos titulares de dados pessoais.

Art. 2º A Lei nº 13.709, de 14 de agosto de 2018, passa a vigorar acrescida do seguinte artigo 54-A:

"Art. 54-A Os agentes de tratamento deverão divulgar, em veículos de comunicação social de grande circulação e em suas páginas e perfis nos provedores de aplicações, qualquer incidente de segurança que possa acarretar risco ou dano relevante aos titulares, conforme critérios estabelecidos pela Autoridade Nacional de Proteção de Dados Pessoais (ANPD). A comunicação à ANPD deverá ser realizada no prazo de três dias úteis, contado do conhecimento do incidente,

incluindo ampla divulgação quando necessário para mitigar riscos ou danos.

§ 1º A comunicação de incidentes de segurança será obrigatória quando o incidente puder afetar significativamente interesses e direitos fundamentais dos titulares e envolver, pelo menos, um dos seguintes critérios:

I - dados pessoais sensíveis;

II - dados de crianças, de adolescentes ou de idosos;

III - dados financeiros;

IV - dados de autenticação em sistemas;

V - dados protegidos por sigilo legal, judicial ou profissional;

VI - dados em larga escala.

§ 2º A comunicação à ANPD deverá conter, no mínimo, as seguintes informações:

I - descrição da natureza e categoria dos dados pessoais afetados;

II - número de titulares afetados, discriminando, quando aplicável, o número de crianças, adolescentes ou idosos;

III - medidas técnicas e de segurança adotadas antes e após o incidente;

IV - riscos relacionados ao incidente e possíveis impactos aos titulares;

V - medidas adotadas para reverter ou mitigar os efeitos do incidente;

VI - data do incidente e da ciência pelo controlador;

VII - dados de contato do encarregado pelo tratamento de dados pessoais.

§ 3º Nos casos em que a comunicação direta aos titulares não for suficiente para mitigar riscos ou danos, os agentes de tratamento deverão divulgar o incidente em veículos de comunicação social de grande circulação e em suas páginas e perfis nos provedores de aplicações.

§ 4º Os agentes de tratamento deverão manter registro dos incidentes de segurança por um período mínimo de cinco anos, contendo:

I - data de conhecimento do incidente;

II - descrição das circunstâncias do incidente;

III - natureza e categoria dos dados afetados;

IV - número de titulares afetados;

V - avaliação dos riscos e danos potenciais;

VI - medidas de correção e mitigação adotadas;

VII - forma e conteúdo da comunicação à ANPD e aos titulares;

VIII - motivos da ausência de comunicação, quando for o caso.

§ 5º O descumprimento das obrigações estabelecidas neste artigo sujeitará os agentes de tratamento às sanções previstas no art. 52 desta Lei, e poderá resultar na instauração de processo administrativo sancionador pela ANPD para apurar a ocorrência de infrações e aplicar as sanções cabíveis, incluindo advertência, multa, bloqueio e eliminação dos dados pessoais relacionados ao

incidente, conforme regulamentação específica." *(NR)*

Art. 3º Esta lei entra em vigor na data da sua publicação.

JUSTIFICAÇÃO

Um dos problemas mais recorrentes na sociedade da informação e na economia digital é a quantidade de dados pessoais que circulam entre empresas e governos. Não é raro lermos notícias que relatam enormes volumes de dados de titulares vazados ou mesmo à venda no mercado negro.

Nesse cenário, o usuário muitas vezes não é informado sobre quando e quais dados seus foram objeto de um incidente de segurança e, por isso, não é capaz de tomar as providências e precauções que naturalmente tomaria.

Conforme previsto no § 3º do art. 37 da Constituição Federal, a lei estabelecerá os direitos dos usuários de serviços públicos em todo o País, incluindo, por exemplo, o acesso "a registros administrativos e a informações" (inciso II do § 3º do art. 37). A Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), representa um marco na proteção dos dados pessoais no Brasil, estabelecendo princípios e regras para assegurar a privacidade e a proteção dos dados dos cidadãos.

Recentes incidentes de vazamento de dados pessoais evidenciam a necessidade de aperfeiçoar a LGPD para garantir maior segurança e transparência na comunicação desses incidentes. Em abril de 2021, a Consultoria Legislativa da Câmara dos Deputados, através dos consultores Claudio Nazareno, Guilherme Pinheiro, Thiago Soares, Adriano Nóbrega e Cassiano Negrão, elaborou a Nota Técnica intitulada "Consequências dos Megavazamentos de Dados para os Cidadãos", destacando os impactos negativos significativos que tais vazamentos podem

causar aos indivíduos. O estudo está disponível em: Nota Técnica – Consequências dos Megavazamentos de Dados para os Cidadãos.

Além disso, a Autoridade Nacional de Proteção de Dados (ANPD) publicou a Resolução nº 15/2024, que aprovou o Regulamento de Comunicação de Incidente de Segurança (RCIS). Este regulamento estabelece procedimentos detalhados para a comunicação de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares de dados, promovendo a adoção de boas práticas de governança e segurança de dados pessoais.

Nesse sentido, entendemos ser oportuno que os agentes de tratamento, ou seja, tanto controladores como operadores, nos termos da LGPD, sejam obrigados a divulgar em veículos de comunicação social de grande circulação, bem como em suas páginas e perfis nos provedores de aplicações, todo incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Ademais, previmos, na presente iniciativa, que os agentes de tratamento devem informar o fato, tão logo ocorrido, para a Autoridade Nacional de Proteção de Dados Pessoais (ANPD).

A necessidade de transformar esses dispositivos em norma legal, aprovada pelo Congresso Nacional, se justifica pela importância de conferir maior legitimidade e segurança jurídica às medidas de proteção de dados pessoais. Embora a Resolução nº 15/2024 da ANPD tenha estabelecido diretrizes importantes, a sua consolidação em uma norma federal aprovada pelo Congresso Nacional fortalece o cumprimento e a fiscalização dessas disposições.

Para a formulação deste projeto, aproveitou-se do estudo detalhado elaborado pela Consultoria Legislativa da Câmara dos Deputados e das diretrizes estabelecidas pela Resolução nº 15/2024 da ANPD. Ao consolidar essas disposições em uma norma federal, asseguramos que os direitos dos titulares de dados sejam respeitados e observados conforme as diretrizes estabelecidas pela LGPD.

Desse modo, é possível emprestar maior transparência a casos de vazamento de dados ou outros incidentes de segurança semelhantes,

munindo o titular e a própria ANPD do conhecimento e dos meios para remediar os prejuízos deles decorrentes.

Dessa forma, a inclusão dessas medidas na LGPD reforça a importância da proteção de dados pessoais no Brasil, assegurando que os agentes de tratamento de dados adotem práticas transparentes e responsáveis na comunicação de incidentes de segurança. Além disso, a obrigatoriedade de manter registros detalhados de incidentes e a definição de penalidades claras para o descumprimento das obrigações previstas promovem a responsabilidade e a prestação de contas.

Diante do exposto, e da importância fundamental do tema em questão, conclamamos os nobres pares desta Casa para aprovar o presente projeto de lei.

Sala das Sessões, em de de 2024.

Deputado **ULISSES GUIMARÃES**

CÂMARA DOS DEPUTADOS
CENTRO DE DOCUMENTAÇÃO E INFORMAÇÃO – CEDI
Coordenação de Organização da Informação Legislativa – CELEG

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018	https://normas.leg.br/?urn=urn:lex:br:federal:lei:2018-08-14;13709

PROJETO DE LEI N.º 3.457, DE 2024

(Da Sra. Antônia Lúcia)

Acrescenta artigo à Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), para dispor sobre a proteção de contas de redes sociais invadidas e os direitos dos consumidores afetados.

DESPACHO:
APENSE-SE À(AO) PL-1876/2023.

CÂMARA DOS DEPUTADOS
Gabinete da Deputada Antônia Lúcia

PROJETO DE LEI Nº , DE 2024

Acrescenta artigo à Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), para dispor sobre a proteção de contas de redes sociais invadidas e os direitos dos consumidores afetados.

O CONGRESSO NACIONAL decreta:

Art. 1º A Lei nº 13.709, de 14 de agosto de 2018, passa a vigorar acrescida do seguinte artigo:

"Art. 43-A. Em casos de invasão de contas de redes sociais, caberá ao controlador de dados, em parceria com a plataforma de rede social, adotar medidas imediatas para:

I. Restabelecer o acesso seguro à conta invadida, assegurando a verificação de identidade do titular dos dados;

II. Notificar o titular dos dados e as autoridades competentes sobre a invasão e as medidas adotadas para contenção e resolução do incidente, no prazo máximo de 24 horas;

III. Assegurar que quaisquer dados pessoais coletados ou expostos durante a invasão sejam removidos ou neutralizados de forma segura, evitando sua utilização para fins ilícitos;

IV. Facilitar ao titular dos dados o acesso a canais de comunicação direta para relatar incidentes e solicitar informações sobre o andamento da resolução do problema;

V. Prover ao titular dos dados informações claras e precisas sobre os direitos garantidos pela LGPD, bem como as possíveis ações legais cabíveis em casos de prejuízo decorrente da invasão.

O não cumprimento das disposições deste artigo sujeitará o controlador a sanções inistrativas previstas nesta Lei, além de responsabilidade civil pelos danos causados tular dos dados.

§2º O titular dos dados que tiver sua conta invadida terá o direito de solicitar a revisão das políticas de segurança da plataforma de rede social, com vistas à prevenção de novas invasões.

§3º Em casos de danos materiais ou morais comprovados, o titular dos dados terá direito à reparação de acordo com o disposto nesta Lei."

Art. 2º Esta Lei entra em vigor na data de sua publicação.

Justificação:

A era digital trouxe inúmeros avanços e benefícios à sociedade, mas também impôs desafios significativos, especialmente no que se refere à segurança dos dados pessoais. Entre as ameaças mais alarmantes e recorrentes estão as invasões de contas em redes sociais, em especial no Instagram, que têm se multiplicado em uma velocidade preocupante. Tais invasões não apenas comprometem a privacidade dos usuários, mas também expõem dados pessoais e sensíveis, gerando um efeito cascata de fraudes, extorsões e outros crimes, com potencial de impactar a vida financeira, profissional e emocional das vítimas.

Atualmente, as plataformas digitais, na maioria das vezes, limitam-se a fornecer orientações gerais de segurança, muitas vezes insuficientes para evitar tais violações. Quando uma conta é invadida, a responsabilidade e o ônus de resolver o problema recaem quase que integralmente sobre o usuário, que, por sua vez, enfrenta uma jornada árdua e desgastante para recuperar seus dados e restabelecer a sua segurança digital.

Este cenário revela uma lacuna significativa na proteção dos consumidores, que, apesar de amparados pela Lei Geral de Proteção de Dados Pessoais (LGPD), ainda enfrentam dificuldades na busca por reparação e justiça em casos de invasões. O presente Projeto de Lei surge com o propósito de preencher essa lacuna, ampliando as responsabilidades dos controladores de dados e das plataformas digitais no que tange à segurança das contas e à resposta rápida e eficaz em casos de invasão.

A proposta visa assegurar que os consumidores afetados tenham seus direitos resguardados de forma ágil, impondo às plataformas digitais a obrigação de implementar mecanismos de proteção mais robustos, bem como procedimentos de recuperação de contas e reparação de danos mais céleres e transparentes. Além disso, busca-se responsabilizar diretamente as plataformas em casos onde a segurança dos dados tenha sido comprometida por falhas ou omissões em suas políticas de proteção.

Diante do aumento exponencial dos crimes digitais e das invasões de contas, é imprescindível que o Poder Legislativo atue de forma proativa, assegurando que os direitos dos consumidores sejam efetivamente protegidos, e que as plataformas digitais sejam corresponsáveis pela integridade e segurança dos dados de seus usuários.

Projeto de Lei, portanto, representa um passo crucial na proteção dos direitos dos

consumidores no ambiente digital, fortalecendo o arcabouço jurídico nacional e oferecendo uma resposta adequada aos desafios impostos pela era digital.

Brasília, de 2024

Sala das Comissões

Antonia Lucia
Dep. Federal
Republicanos/AC

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018	https://normas.leg.br/?urn=urn:lex:br:federal:lei:201808-14;13709

COMISSÃO DE COMUNICAÇÃO

PROJETO DE LEI Nº 1.876, DE 2023

Apensados: PL nº 2.138/2024, PL nº 272/2024 e PL 3.457/2024

Altera a Lei nº 13.709, de 14 de agosto de 2018, para obrigar a divulgação de incidentes de segurança de dados pessoais em veículos de comunicação social.

Autor: Deputado MARCOS TAVARES

Relator: Deputado JADYEL ALENCAR

I - RELATÓRIO

Tramita nesta Comissão o Projeto de Lei nº 1.876, de 2023, de autoria do Deputado Marcos Tavares, que altera a Lei nº 13.709, de 14 de agosto de 2018, com o fim de obrigar controladores e operadores de tratamento de dados pessoais a divulgarem incidentes de segurança de dados em veículos de comunicação social.

A proposta insere novo dispositivo determinando que agentes de tratamento divulguem, em veículos de comunicação social de grande circulação e em suas páginas e perfis, qualquer incidente de segurança com potencial de acarretar em risco ou dano relevante aos titulares. Ademais, ficam os agentes de tratamento também obrigados a informar o ocorrido à Autoridade Nacional de Proteção de Dados Pessoais – ANPD.

Em 23/02/2024, foi apensado o PL 272/2024, de autoria do deputado Júnior Mano. A proposta estabelece o prazo de 5 dias úteis, a contar da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, para que a Administração Pública, por meio do órgão ou entidade responsável pela irregularidade, no âmbito da União, Estados, Distrito Federal e Municípios, publique com destaque nas páginas de seus sítios

oficiais um comunicado informando sobre o incidente. Além disso, a iniciativa legislativa exige que o comunicado permaneça acessível ao público pelo prazo mínimo de 90 dias, e obriga a ANPD a enviar a todos os usuários do serviço mensagem informando aos titulares dos dados acerca do incidente de segurança.

Já em 17/07/2024, foi a vez do PL 2138/2024, de autoria do Deputado Ulisses Guimarães, ser apensado à matéria principal. O projeto estabelece que os agentes de tratamento de dados devem comunicar qualquer incidente que possa causar risco ou dano relevante aos titulares, divulgando-o em veículos de comunicação de grande circulação e em suas plataformas digitais. A comunicação à Autoridade Nacional de Proteção de Dados (ANPD) deve ser feita em até três dias úteis, contendo informações detalhadas sobre o incidente, como a natureza dos dados afetados, o número de titulares envolvidos e as medidas adotadas para mitigar os riscos. Caso a comunicação direta aos titulares seja insuficiente para reduzir os danos, a ampla divulgação pública também será necessária. O descumprimento dessas obrigações pode resultar em sanções administrativas, como advertências e multas.

Por fim, em 21/10/2024, foi apensado o PL 3.457/2024, de autoria da deputada Antônia Lúcia, que propõe a inclusão do artigo 43-A na Lei Geral de Proteção de Dados Pessoais (LGPD) para reforçar a proteção dos usuários cujas contas de redes sociais foram invadidas. O texto exige que os controladores de dados, em conjunto com as plataformas, tomem medidas imediatas para restaurar o acesso seguro, notificar os usuários e autoridades sobre a invasão e proteger os dados expostos. Além disso, o PL estabelece que as plataformas devem disponibilizar canais diretos para comunicação e suporte aos usuários afetados e garante o direito à reparação em casos de danos comprovados. A proposta também impõe sanções para controladores que não cumprirem essas obrigações, visando fortalecer a segurança digital e a confiança dos consumidores.

A matéria foi distribuída para análise de mérito às Comissões de Comunicação e de Constituição e Justiça e de Cidadania, cabendo a esta última, ainda, análise quanto à constitucionalidade e juridicidade da matéria nos termos do art. 54, do Regimento Interno da Câmara dos Deputados - RICD.

O regime de tramitação é o ordinário e, ao fim do prazo regimental, não foram apresentadas emendas à matéria.

É o Relatório.

II - VOTO DO RELATOR

A presente proposta de alteração da Lei Geral de Proteção de Dados Pessoais (LGPD) responde aos novos desafios impostos pelo uso crescente de decisões automatizadas no tratamento de dados pessoais. A digitalização acelerada de serviços públicos e privados tem ampliado a adoção de sistemas automatizados para tomar decisões que impactam diretamente a vida dos indivíduos, como concessão de crédito, triagem de currículos, liberação de benefícios, diagnósticos preliminares, entre outros. Em muitos desses casos, os titulares não compreendem os critérios utilizados, tampouco dispõem de meios efetivos para contestar os resultados produzidos.

Parte desses sistemas opera com base em regras fixas. Outros, mais complexos, utilizam técnicas de aprendizado de máquina e inteligência artificial, com alto grau de opacidade e difícil auditabilidade. Em ambos os casos, a tomada de decisão integralmente automatizada pode trazer impactos à direitos e à esfera jurídica dos destinatários, afetando também sua autonomia quando houver opacidade quanto aos critérios de decisão que possam dificultar sua contestação ou revisão, além de riscos a direitos fundamentais em dimensão coletiva, por exemplo, quando sistemas de decisão automatizada, largamente aplicados podem resultar em efeitos discriminatórios.

Embora o caput do art. 20 da LGPD já reconheça ao titular o direito à revisão de decisões tomadas exclusivamente por meios automatizados, o dispositivo carece de critérios normativos que orientem as hipótese de revisão humana que pode se mostrar necessária para a garantia substantiva de direitos.

Nesse sentido, o § 4º proposto supre essa lacuna ao estabelecer que a revisão humana será obrigatória sempre que a decisão

automatizada produzir consequências negativas modificativas, impeditivas ou extintivas de direitos, ou gerar impacto significativo equivalente ao titular, desde que seja tecnicamente viável e compatível com o tipo de aplicação envolvida. A redação proposta vincula a exigência de revisão humana à presença de efeitos jurídicos imediatos ou impactos significativamente similares, o que confere densidade prática ao princípio da precaução substantiva, conforme formulado por Juliano Maranhão (2025). 1 Ou seja, não se trata de adotar um procedimento geral de revisão humana, mas circunscrevê-la às hipóteses cabíveis conforme o tipo de decisão automatizada e quando houver efetivo impacto sobre a esfera individual. Com isso se compatibiliza a evolução da tecnologia com a proteção de direitos fundamentais.

Para garantir que a revisão humana seja aplicada de forma efetiva e proporcional, o §5º estabelece a competência da Autoridade Nacional de Proteção de Dados (ANPD) para definir, por meio de regulamentação prévia, os tipos de decisões automatizadas que comportam revisão por pessoa natural. Essa diretriz considera o nível de risco envolvido, o porte do agente de tratamento, o contexto de uso do sistema e o estágio de desenvolvimento tecnológico. Ao prever essa competência normativa, o dispositivo busca oferecer segurança jurídica, viabilidade técnica e evita tanto a exigência desnecessária de revisão em aplicações de baixo impacto, quanto a omissão em cenários de maior potencial lesivo.

Complementarmente, os §§ 1º e 2º introduzidos no art. 22 da LGPD buscam consolidar mecanismos de tutela coletiva e reforçar o papel do Ministério Público na proteção de titulares contra discriminações sistêmicas ou abusos decorrentes de sistemas automatizados.

A proposta autoriza o Ministério Público, no curso de ações coletivas de reparação em juízo, a requerer cautelarmente o fornecimento pelos controladores de:

- informações pertinentes sobre as decisões automatizadas (inciso I);
- relatórios de transparência que assegurem grau mínimo de inteligibilidade da lógica decisória (inciso II); e

- relatórios sobre as práticas de governança e mitigação de riscos discriminatórios (inciso III).

Esses instrumentos visam a superar o atual descompasso entre o avanço tecnológico e a capacidade de fiscalização e responsabilização institucional, muitas vezes obstaculizadas pela complexidade técnica e pela assimetria informacional.

O § 2º ainda prevê que, caso o controlador não apresente informações suficientes para a compreensão dos efeitos discriminatórios e de suas origens, o juízo poderá determinar a inversão do ônus da prova, em consonância com o art. 42, §2º da LGPD e o art. 373, §1º do Código de Processo Civil. Essa medida busca reequilibrar as relações processuais, favorecendo a proteção de titulares estruturalmente vulneráveis diante da opacidade algorítmica.

Em síntese, o projeto fortalece os pilares de transparência, responsabilidade e governança no uso de sistemas automatizados, alinhando-se às diretrizes internacionais e

Nesse sentido, oferecemos voto pela **APROVAÇÃO** do Projeto de Lei nº 1.876, de 2023, 2.138/2024, PL nº 272/2024 e 3.457/2024 **na forma do SUBSTITUTIVO** que a seguir apresentamos.

Sala da Comissão, em de de 2025.

Deputado JADYEL ALENCAR
Relator

COMISSÃO DE COMUNICAÇÃO

SUBSTITUTIVO AO PROJETO DE LEI Nº 1.876, DE 2023

Altera a Lei nº 13.709, de 14 de agosto de 2018, para obrigar a divulgação de incidentes de segurança de dados pessoais em veículos de comunicação social.

O Congresso Nacional decreta:

Art. 1º Esta lei altera a Lei nº 13.709, de 14 de agosto de 2018, para obrigar a divulgação de incidentes de segurança de dados pessoais em veículos de comunicação social.

Art. 2º A Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), passa a vigorar com as seguintes alterações:

Art. 20 .....

.....

§ 4º Por solicitação do titular afetado, a revisão de que trata o caput deste artigo deverá ser realizada por pessoa natural, quando compatível com o tipo de aplicação e o estado da arte da tecnologia, desde que a decisão produza consequências negativas modificativas, impeditivas ou extintivas de direitos ao titular de dados, ou que o afete significativamente, de forma similar.

§5º O exercício do direito previsto no §4º dependerá de regulamentação da autoridade nacional sobre tipos de decisão automatizadas compatíveis com a revisão humana, considerando o estado da arte da tecnologia. (NR)

Art. 22 .....

§ 1º Em ações coletivas de reparação em juízo, observado o disposto na legislação pertinente, respeitado o devido processo legal, o Ministério Público poderá requerer ao juízo, cautelarmente, de modo fundamentado, a apresentação pelo controlador de:

I - informações sobre o conjunto das decisões automatizadas adotadas pelo controlador que sejam pertinentes ao objeto da ação;

II - relatório de transparência pelo controlador que permita grau suficiente de inteligibilidade da decisão automatizada;

III - relatório sobre as medidas de governança adotadas para mitigação dos riscos de efeitos discriminatórios decorrentes do sistema de decisões automatizadas adotado.

§ 2º O fornecimento das informações indicadas nos incisos do parágrafo anterior de modo insuficiente para a compreensão mínima dos efeitos discriminatórios e de suas possíveis fontes, considerando o ciclo de vida do sistema de decisão automatizada, poderá ensejar a inversão do ônus da prova em favor dos titulares, nos termos do §2º do art. 42 desta Lei e do §1º do art.373 do Código de Processo Civil Brasileiro. (NR)

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

Sala da Comissão, em de de 2025.

Deputado JADYEL ALENCAR
Relator

Câmara dos Deputados

COMISSÃO DE COMUNICAÇÃO

PROJETO DE LEI Nº 1.876, DE 2023

III - PARECER DA COMISSÃO

A Comissão de Comunicação, em reunião extraordinária realizada hoje, mediante votação ocorrida por processo simbólico, concluiu pela aprovação do Projeto de Lei nº 1.876/2023, do PL 272/2024, do PL 2138/2024, e do PL 3457/2024, apensados, com Substitutivo, nos termos do Parecer do Relator, Deputado Jadyel Alencar.

Registraram presença à reunião os seguintes membros:

Julio Cesar Ribeiro - Presidente, Amaro Neto, David Soares e Paulo Magalhães - Vice-Presidentes, André Figueiredo, Antonio Andrade, Bia Kicis, Capitão Alberto Neto, Cezinha de Madureira, Dimas Gadelha, Fábio Teruel, Jadyel Alencar, Juscelino Filho, Ossesio Silva, Rodrigo da Zaeli, Rodrigo Estacho, Albuquerque, Alex Manente, Bibo Nunes, Delegado Paulo Bilynskyj, Franciane Bayer, Gustavo Gayer, Lucas Ramos, Luciano Alves, Marangoni, Marcos Soares, Pastor Diniz e Rosana Valle.

Sala da Comissão, em 20 de agosto de 2025.

Deputado JULIO CESAR RIBEIRO
Presidente

COMISSÃO DE COMUNICAÇÃO

SUBSTITUTIVO ADOTADO AO PROJETO DE LEI Nº 1876, DE 2023
Apensados PL 272/2024, PL 2138/2024 e PL 3475/2024

Altera a Lei nº 13.709, de 14 de agosto de 2018, para obrigar a divulgação de incidentes de segurança de dados pessoais em veículos de comunicação social.

O Congresso Nacional decreta:

Art. 1º Esta lei altera a Lei nº 13.709, de 14 de agosto de 2018, para obrigar a divulgação de incidentes de segurança de dados pessoais em veículos de comunicação social.

Art. 2º A Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), passa a vigorar com as seguintes alterações:

Art. 20 .....

§ 4º Por solicitação do titular afetado, a revisão de que trata o caput deste artigo deverá ser realizada por pessoa natural, quando compatível com o tipo de aplicação e o estado da arte da tecnologia, desde que a decisão produza consequências negativas modificativas, impeditivas ou extintivas de direitos ao titular de dados, ou que o afete significativamente, de forma similar.

§5º O exercício do direito previsto no §4º dependerá de regulamentação da autoridade nacional sobre tipos de decisão automatizadas compatíveis com a revisão humana, considerando o estado da arte da tecnologia. (NR)

Art. 22 .....

§ 1º Em ações coletivas de reparação em juízo, observado o disposto na legislação pertinente, respeitado o devido processo legal, o Ministério Público poderá requerer ao juízo, cautelarmente, de modo fundamentado, a apresentação pelo controlador de:

I - informações sobre o conjunto das decisões automatizadas adotadas pelo controlador que sejam pertinentes ao objeto da ação;

II - relatório de transparência pelo controlador que permita grau suficiente de inteligibilidade da decisão automatizada;

III - relatório sobre as medidas de governança adotadas para mitigação dos riscos de efeitos discriminatórios decorrentes do sistema de decisões automatizadas adotado.

§ 2º O fornecimento das informações indicadas nos incisos do parágrafo anterior de modo insuficiente para a compreensão mínima dos efeitos discriminatórios e de suas possíveis fontes, considerando o ciclo de vida do sistema de decisão automatizada, poderá ensejar a inversão do ônus da prova em favor dos titulares, nos termos do §2º do art. 42 desta Lei e do §1º do art.373 do Código de Processo Civil Brasileiro. (NR)

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

Sala da Comissão, em 20 de agosto de 2025.

Deputado **Julio Cesar Ribeiro**
Presidente