CONSELHO DIGITAL
contato@conselhodigital.org.br

PL 3343-2020 NT 11.05.2023

versão ajustada em 11.05.2023

Resumo Executivo

PL 3.343/2020 | CCOM

REJEIÇÃO

Image not found or type unknown
Image3

AUTOR: DEP. DAYANE PIMENTEL (UNIÃO/BA)

RELATOR: DEP. MAURÍCIO MARCON (PODE/RS)

TRAMITAÇÃO: CCOM (PRONTA PARA PAUTA NA COMISSÃO DE COMUNICAÇÃO)

EMENTA: Recursos de Segurança em Aplicativos de Mensageria

TAGS: Privacidade, vigilância e dados, Comunicação massiva

SE A PROPOSIÇÃO FOR APROVADA

- Prejudicará a experiência dos usuários, pois a dinâmica da plataforma será completamente alterada.
- Serão necessárias alterações estruturais nos aplicativos.
- Gerará riscos à privacidade e ao sigilo das comunicações.
- Haverá intervenção excessiva nas atividades das plataformas e aumento dos custos do negócios.

O PL 3343/2020 dispõe sobre a responsabilidade de aplicativo de troca de mensagens quanto à segurança de acesso e a privacidade das informações, obrigando os aplicativos a ***(i)***

oferecer recursos de segurança, de fácil compreensão, para impedir a clonagem da conta, garantir o sigilo das mensagens e impedir o armazenamento não autorizado e ***(ii)*** ter ferramentas para identificar o envio de mensagens massivas, comunicando ao usuário a tentativa de realização dessas operações.

A PROPOSTA É IMPRECISA E DESNECESSÁRIA

O PL é impreciso e **não eleva o grau de proteção e segurança** no espaço virtual. O que seria considerado clonagem de conta? Hoje, criminosos utilizam diversos artifícios para dar golpes – acessam as contas de terceiros ou utilizam um número diverso e simulam ser um usuário. Muitos desses mecanismos independem de qualquer violação à segurança das plataformas.

Os aplicativos já possuem **incentivos orgânicos para investir em ferramentas de segurança** – quanto mais seguro e sigiloso é o aplicativo, mais atrativo para os usuários. Essas plataformas também têm mecanismos modernos de segurança – como criptografia de ponta-a-ponta e verificação em duas etapas – e realizam campanhas informativas para seus usuários sobre como evitar golpes e recuperar suas contas.

A atual legislação já é robusta e garante um elevado grau de proteção ao usuário, assegurando sua privacidade, o sigilo das comunicações e a proteção aos dados pessoais – direitos previstos em diversos diplomas legais como na Constituição Federal, no Marco Civil da Internet (MCI) e na Lei Geral de Proteção de Dados Pessoais (LGPD).

INTERVENÇÃO EXCESSIVA

O PL desconsidera os limites técnicos das ferramentas, impõe alterações técnicas, aumenta os custos do negócios e **burocratiza a atividade**. É intervenção excessiva, que viola ***(i)*** o princípio constitucional da livre iniciativa; ***(ii)*** a liberdade dos modelos de negócios promovidos na Internet (art. 3º, VIII, MCI) e ***(iii)*** a Lei de Liberdade Econômica, que consagrou a liberdade no exercício de atividades econômicas e a intervenção mínima e subsidiária do Estado.

A escolha de quais funcionalidades serão oferecidas por cada aplicativo é uma **decisão privada, baseada no modelo e estratégia de negócios** de cada empresa. Não é razoável buscar responsabilizar as plataformas por ilegalidades cometidas por terceiros, sobre as quais não têm qualquer controle.

VIOLA O MARCO CIVIL DA INTERNET

O PL viola o MCI ao impor uma espécie de **obrigação de monitoramento** aos aplicativos

de mensagem, que deverão “manter procedimentos de identificação de transações envolvendo volumes expressivos de envio de dados ou sua distribuição a grande número de destinatários”, podendo prejudicar a liberdade de expressão e gerar censura.

É importante considerar que **o envio massivo de mensagens nem sempre é negativo**. Na verdade, é uma ferramenta utilizada por diversos empreendedores e órgãos do Estado, que facilita as comunicações e a interação com seu público alvo.

INVIABILIDADE

A obrigação de controle do envio de mensagens sequer é viável, pois seria necessário acesso ao teor das comunicações. Muitos aplicativos, buscando assegurar a privacidade dos usuários, utilizam **criptografia de ponta-a-ponta**, uma ferramenta de proteção que anonimiza os dados trafegados – ao enviar uma mensagem, os dados são convertidos em um texto embaralhado, que só pode ser decodificado com uma chave secreta, de forma que nem mesmo as plataformas têm acesso ao seu teor.

O texto também obriga que o remetente seja notificado da tentativa de envio de volume expressivo de dados ou sua distribuição a um grande número de destinatários. Para tanto, seriam necessárias alterações de produto, que podem gerar elevados custos e serem inviáveis, sobretudo para startups e pequenas plataformas.

PL 3.343/2020 | CONCLUSÃO

REJEIÇÃO

A internet deve continuar sendo uma rede aberta, livre e plural. O PL é excessivamente intervencionista e pode prejudicar o desenvolvimento de aplicações que têm se tornado extremamente importantes para os brasileiros.

Este resumo executivo foi elaborado pela equipe técnica do Instituto Cidadania Digital no cumprimento de sua função de secretariado-executivo da Frente Parlamentar da Economia e Cidadania Digital. Para maiores informações consulte nossa equipe. Para assessores e parlamentares receberem os resumos executivos, por favor se cadastrem em nossa lista de transmissão através do contato com nossa equipe.

Felipe Melo França ……. franca@cidadaniadigital.in
……. 11 974.170.905

Roberta Jacadá ……. roberta@cidadaniadigital.in
……. 61 981.339.816

Rebeca Mota ……. rebeca@cidadaniadigital.in
……. 61 981.008.822

Kézia Costa …….. kezia@cidadaniadigital.in
……. 61 993.675.357

Walysson Barros ……. barros@cidadaniadigital.in
…….. 61 995.544.932

Yngrid Nascimento …….. yngrid@cidadaniadigital.in
……. 61 994.192.264

Image2

Image1

www.frentedigital.org

cidadaniadigital.in

Image not found or type unknown

Image not found or type unknown

Category

1. Conteúdo Restrito

Date
08/09/2024
Date Created
11/01/2024