CONSELHO DIGITAL
contato@conselhodigital.org.br

PL 113-2020 NT 11.12.23

versão ajustada em 11.12.2023

Resumo Executivo

PL 113/2020 | CCDD | SF

REJEIÇÃO DO PROJETO E DO SUBSTITUTIVO

AUTOR: Sen. ÂNGELO CORONEL – PL/SP

RELATOR: Sen**.** ASTRONAUTA MARCOS PONTES – PSB-BA

EMENTA: Altera a Lei 12.965/2014 – MCI – para determinar o cadastramento dos usuários pelos provedores de internet.

PARA ENTENDER MELHOR:

- A Lei Geral de Proteção de Dados exige tratamento que resguarde os dados e informações dos usuários dos meios digitais.
- O Marco Civil da Internet é uma Lei que visa garantir que os usuários de internet tenham resguardados seus direitos básicos no mundo digital e que as empresas do setor atuem justamente para garanti-los.

O PL 113/2020 foi apresentado no dia 05/02/2020 ao Senado Federal, pelo Senador Ângelo Coronel, visando a inclusão do Art. 15-A à Lei 12.965/2014 – Marco Civil da Internet.

A inclusão deste artigo visa estabelecer aos provedores de aplicações de internet a obrigatoriedade de solicitarem que seus usuários se registrem e o façam através do cadastro do CPF ou CNPJ.

O PL foi distribuído originalmente à Comissão de Ciência, Tecnologia, Inovação e Informática – CCTI, tendo sido redistribuído à Comissão criada no Senado com competência material para análise da matéria, qual seja, Comissão de Comunicação e Direito Digital.

Em 22 de novembro o Relator, Senador Astronauta Marcos Pontes apresentou relatório com voto pela **aprovação do Projeto na forma do Substitutivo por ele apresentado.**

O Substitutivo apresenta uma série de mudanças ao Projeto original do PL 113/2023 e, consequentemente na Lei 12.965/2014, inclusive na ementa que passa a descrever que dispõe sobre "guarda e disponibilização de registros de conexão e de acesso de provedores na internet".

O novo texto acabou por alterar o escopo do PL original, apresentando uma série de pontos questionáveis em relação à garantia da intimidade e privacidade dos usuários e de concordância com ditames internacionais sobre o tema.

INSERIR A GEOLOCALIZAÇÃO COMO PARTE DO REGISTRO DE ACESSO A APLICAÇÕES DE INTERNET COLOCA O BRASIL EM OPOSIÇÃO AOS PADRÕES INTERNACIONAIS DE PRIVACIDADE.

Os padrões internacionais de privacidade e proteção de dados são fundamentais para garantir que as práticas de coleta, armazenamento e processamento de dados pessoais sejam realizadas de maneira segura e ética. Há vários regulamentos e diretrizes internacionais que estabelecem esses padrões e que, **com a aprovação do PL nos termos do Substitutivo, fará com que nossa legislação esteja destoante dos comparativos internacionais**.

Veja-se o Regulamento Geral de Proteção de Dados (GDPR) da **União Europeia**, que é talvez o mais influente e abrangente regulamento de proteção de dados em vigor. Implementado em 2018, o GDPR estabelece diretrizes rigorosas para a coleta e processamento de dados pessoais de cidadãos da UE, **incluindo requisitos para consentimento, direitos de acesso** e exclusão de dados, e transferências internacionais de dados. Uma de suas características marcantes é o seu alcance extraterritorial, pois se aplica a qualquer organização, em qualquer lugar do mundo, que processe dados de cidadãos da UE.

Além disso, a Convenção 108 do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, conhecida como Convenção 108, é o primeiro tratado internacional juridicamente vinculativo sobre privacidade e proteção de dados. Ela estabelece diretrizes para a coleta e processamento de dados pessoais, **assegurando** o respeito aos direitos humanos e **às liberdades fundamentais**, especialmente o direito à privacidade.

Destoando do previsto na convenção, o Substitutivo fere os direitos à intimidade e

privacidade ao estabelecer que deva fazer parte do registro de acesso a aplicações da internet os dados referentes à **geolocalização**. Este dado **não deve compor** os dados de registro e que podem ser solicitados de forma simples e sem justificativa por autoridades que não as judiciais.

A consideração de que a geolocalização seria dado a ser disponibilizado em requisições feitas por autoridades administrativas e membros de Ministério Público e Delegados, afronta esta Convenção e as demais diretrizes internacionais.

Também mencionam-se aqui os **Princípios de Privacidade** da **Organização para Cooperação e Desenvolvimento Econômico** (OCDE): A OCDE formulou princípios que servem **como diretrizes para políticas de privacidade em seus países membros**. Estes princípios incluem **limitações à coleta de dados**, qualidade dos dados, **finalidade**, segurança, transparência, participação individual e responsabilidade.

Mais uma vez a comunidade internacional deixa clara a necessidade de limitações à coleta de dados e o dever de uso responsável e finalísticos das informações coletadas.

No mesmo sentido, a **Lei de Privacidade do Consumidor da Califórnia** (CCPA) que embora seja uma legislação estadual dos EUA, tem influência internacional devido à importância econômica da Califórnia, que dispõe contra a geolocalização como dado a ser fornecido sem determinação judicial.

A inclusão de dados de geolocalização em registros de acesso a aplicações de internet, como proposto na emenda ao Marco Civil da Internet, **pode entrar em conflito com esses padrões internacionais, especialmente** no que **diz respeito ao consentimento**, minimização de dados, e direitos dos titulares dos dados. Isso pode criar dificuldades para empresas brasileiras que operam internacionalmente ou que processam dados de indivíduos de países com regulamentações mais rígidas. Além disso, **poderia afetar acordos de transferência de dados internacionais,** cooperação e comércio com países que aderem a esses padrões internacionais.

Resumindo, o Direito Comparado desestimula a inclusão de geolocalização como informação de registro que pode ser requisitada por outros meios que não a determinação judicial.

E, nos casos em que é aceita, há expressa previsão no sentido de que devam os titulares dos dados expressarem consentimento na coleta e disponibilização dos dados, o que **não está previsto no texto do Substitutivo.**

INSERIR A GEOLOCALIZAÇÃO COMO PARTE DO REGISTRO DE ACESSO É TOTALMENTE CONTRÁRIO AOS PRINCÍPIOS E DETERMINAÇÕES GERAIS DA LGPD.

A Lei 13.709/2018 foi amplamente debatida no Congresso Nacional, originada de um amplo debate com participação de diferentes setores da sociedade e que inovou o ordenamento jurídico brasileiro para resguardar a privacidade, intimidade e outros direitos fundamentais da pessoa humana, é **diametralmente oposta** ao que o presente PL pretende implementar.

Os direitos de privacidade de dados arduamente conquistados pela população brasileira serão desconsiderados com a alteração pretendida.

Explicamos, a inclusão de dados de geolocalização nos registros de acesso **ampliaria significativamente a quantidade de dados pessoais coletados,** armazenados e **possivelmente compartilhados**. Isso colide com os princípios de privacidade e proteção de dados estabelecidos pela Lei Geral de Proteção de Dados (LGPD), que **preconiza a minimização da coleta de dados.**

A coleta de dados de geolocalização **exigiria um consentimento explícito e informado do usuário**, conforme determinado pela LGPD. A proposta não deixa claro como esse consentimento seria obtido e gerenciado, o que pode resultar em violações de privacidade.

E parece que resta bastante evidente que este é um tema atinente à coleta de dados e posterior armazenamento e utilização, por isso, deveria ser tratado na Lei Geral de Proteção de Dados e não somente no Marco Civil da Internet.

Caso haja aprovação deste Substitutivo, teremos uma Lei específica sobre o tema que trata a questão de uma forma – LGPD – e outra Lei com escopo interligado, mas não próprio de proteção de dados, impondo outra forma de tratamento de dados – MCI.

Assim, parece adequado que, se for o caso de acréscimo de dados em cadastros ou registros, haja discussão junto à LGPD e esteja de acordo com seus princípios e objetivos basilares.

AUSÊNCIA DE DETERMINAÇÃO JUDICIAL PARA DISPONIBILIZAÇÃO DE DADOS E REGISTROS PESSOAIS: INCOMPATIBILIDADES JURÍDICAS

O Substitutivo prevê que juízes, delegados de polícia, Ministério Público ou autoridade administrativa poderão requerer a qualquer provedor de aplicação os registros de acesso, como alteração pretendida pelo Art.5? do PL.

Parece desarrazoada e impertinente essa possibilidade, afinal, estamos diante de dados

privativos das pessoas, incluindo dados sensíveis,e pretende o PL que autoridades administrativas e o Ministério Público possam requisitá-las a qualquer tempo.

Lembramos que há centenas de autoridades administrativas no Brasil, sendo que encontram-se nas três esferas de governo e muitas delas são competentes para questões que em nada tem a ver com necessidade de fornecimento de dados cadastrais.

Além disso, a **expressão "Ministério Público" mostra-se inadequada**, na medida em que trata-se de uma **Instituição**. A redação adequada parece ser "Promotores e Procuradores de Justiça", **exigindo, portanto, alteração redacional.**

Mas ainda assim, parece que esta previsão pretendida **fere a reserva de jurisdição**, na qual caberia apenas aos Juízes determinarem o fornecimento de dados pessoais por terceiros que o detêm.

Estamos diante de direitos pessoais extremamente importantes e mostra-se adequado e pertinente que **tão somente com determinação judicial se possa acessar e fornecer dados referentes a registros de acesso a aplicações de internet.**

A Constituição Federal, em seu art.5?, garante a inviolabilidade da intimidade e da vida privada, sendo considerado d**ireito e garantia fundamental**, senão vejamos a redação do referido dispositivo:

"X — são **invioláveis** a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;"

Ora, para que não haja violação deste direito intrínseco da pessoa humana no Brasil, exige-se determinação judicial a requisitá-la, quando tal informação estiver na posse de terceiro, ou, quando houver consentimento expresso do seu titular com o compartilhamento de dados.

Ora, se não foi o caso de autorização expressa, a **requisição somente poderá ser feita por autoridade judicial competente,** sob pena de ser inconstitucional a medida e a Lei que a determinou.

A privacidade é um direito fundamental, permitir que autoridades administrativas e policiais acessem dados de geolocalização sem supervisão judicial pode levar a violações desse direito. A **intervenção de um juiz assegura um equilíbrio** entre a **necessidade de investigação** e a **proteção dos direitos individuais.**

Assim, mostra-se inapropriado o Substitutivo do PL 113/2023 que pretende autorizar que "autoridades administrativas", "Delegado de Polícia" e "Ministério Público" requeiram registros de acesso a aplicações de internet.

AUSÊNCIA DE DETERMINAÇÃO JUDICIAL PARA DISPONIBILIZAÇÃO DE DADOS E REGISTROS PESSOAIS : INADEQUAÇÕES

A pretensão de que outras autoridades que não juízes possam determinar a requisição de registros de acesso – incluindo geolocalização – a qualquer provedor de internet não apenas encontra entraves jurídicos, mas éticos, de razoabilidade e de abuso de poder.

Chamamos a atenção para o fato de que sem a supervisão de um juiz, existe um risco maior de **abuso de poder por parte das autoridades**, como a coleta de dados sem justificativa adequada ou por motivações políticas ou pessoais.

A ausência de determinação judicial igualmente fere os princípios da legalidade e da proporcionalidade, já que uma ordem judicial assegura que a requisição de dados seja proporcional e necessária, requisitos imprescindíveis em um Estado Democrático de Direito.

Ademais, é inequívoco que a necessidade de requisição judicial proporciona **segurança jurídica**, uma vez que, oferece uma salvaguarda contra a arbitrariedade, garantindo segurança jurídica tanto para os usuários quanto para os provedores de serviços de internet.

Não parece existir razão para que **qualquer autoridade administrativa** possa **requisitar dados** que dizem respeito à intimidade e privacidade das pessoas. Lembramos que aqui **estamos tratando de dados de acesso, de geolocalização** e **não** apenas de nome e CPF.

Cada prefeitura tem dezenas de secretarias, cada secretaria tem seus departamentos, cada chefe de departamento é uma espécie de autoridade administrativa, afinal, a Lei não delimitou ou conceituou o que entende por autoridade administrativa.

O Brasil possui 5.500 (cinco mil e quinhentos Municípios), cada um deles possui um número elevado de autoridades administrativas, soma-se a este contexto, todas as autoridades das esferas estaduais e federais. Inevitavelmente teremos umas milhares de autoridades administrativas.

Ora, é descabido que autoridades que não precisam de dados como acesso e geolocalização possam determinar que haja fornecimento destes dados.

No mesmo sentido, não parece adequado que qualquer agente do Ministério Público possa determinar a concessão destas informações, afinal, quantos funcionários há no Ministério

Público Federal e nos Ministérios Públicos Estaduais? Milhares também.

E ainda que a intenção do legislador seja a de mencionar promotores de justiça e não Ministério Público como um todo, não há porque promotores determinarem a requisição de informações tão íntimas e privadas como essa, sem que haja aval do juiz.

Além disso, é necessário mencionar que a exigência de uma ordem judicial **assegura** maior **transparência** e **prestação de contas** no processo de coleta de dados. Isso reforça a confiança pública nas instituições e nos processos de aplicação da lei.

Por fim, ainda cabe ressaltar que a necessidade de determinação judicial é uma **forma de proteção contra vigilância massiva,** por quanto a autorização judicial específica para cada caso ajuda a **prevenir** a vigilância massiva e indiscriminada, assegurando que apenas dados relevantes para uma investigação específica sejam coletados.

Diante do exposto, mostra-se **razoável** e **necessário** que **haja determinação judicial** para **concessão dos dados de acesso** por parte dos provedores de aplicação de internet.

DESCABIMENTO AUMENTO DO PRAZO DE DEVER DE MANUTENÇÃO DE REGISTRO DE ACESSO EM AMBIENTE CONTROLADO E DE SEGURANÇA

O Substitutivo apresenta a dilação do prazo de dever de armazenamento dos registros de acesso dos usuários pelos provedores de aplicação da internet de 6 meses para 3 anos. Ora, tal alteração não merece permanecer.

Precisamos primeiramente mencionar a **impossibilidade técnica de manutenção dos registros por prazo tão extenso**. São milhares de acessos por minuto, são milhares de usuários por dias, em diferentes acessos, de diferentes locais e meios. N**ão há como armazenar tamanha quantidade de dados por três anos.**

É tão desproporcional o aumento do prazo que representa um **aumento de 300% do prazo atual**, o que revela a inadequação da medida.

Essa impossibilidade mostra-se ainda mais difícil, pois exige-se que a guarda se dê em ambiente seguro e controlado, o que revela uma incapacidade técnica e operacional.

Não pode prosperar a pretensão do aumento do prazo de armazenamento dos dados dos acessos por três anos, nas condições impostas no PL, vez que é inexequível tal determinação.

DESAFIOS TÉCNICOS E OPERACIONAIS EXIGEM TEMPO E INVESTIMENTO. NECESSIDADE DE VACATIO LEGIS.

Entre outras inadequações do Substitutivo, está o fato de que seria necessária a alta precisão dos sistemas operacionais para detecção precisa da geolocalização. A exatidão da geolocalização, especialmente em ambientes urbanos densos ou em áreas com cobertura limitada de sinal, pode ser um **desafio técnico,** levando a registros imprecisos ou enganosos . De forma que, ao invés de serem úteis, poderiam acabar por gerar confusões e até erros na utilização do dado.

Por outro lado, caso os senhores legisladores entendam pela necessidade desta inclusão, será **preciso a concessão de tempo para a devida adequação** por parte das aplicações de internet.

A previsão de que a Lei deva entrar em vigor em 90 dias da sua publicação mostra-se desarrazoada. As alterações operacionais e adequações técnicas exigem estudo, experimento, investimento não só financeiro, mas especialmente científico e tecnológico.

Por isso, **há a necessidade** de, pelo menos, se determinar um **ano como *vacatio legis***, para fins da necessária implementação das adequações exigidas para inclusão da geolocalização.

PL 113/2023 | CONCLUSÃO

REJEIÇÃO DO SUBSTITUTIVO

O Substitutivo do PL 113/2023 apresentado está eivado incongruências e inadequações que vão no sentido de prejudicar os usuários de internet e estabelecer deveres aos provedores de aplicação de internet que contrariam obrigações a eles impostas pela Constituição Federal e pela Lei Geral de Proteção de Dados. Ainda que o projeto tenha uma boa intenção, trouxe alterações quanto à guarda e disponibilização de registros de conexão e acesso por provedores de internet que não podem ser incorporadas no ordenamento jurídico. Mostra-se necessário que apenas a autoridade judicial tenhapoderes de requisição de registros de acesso, ainda mais, quando se pretende incorporardados de geolocalização nestes registros. Além disso, o próprio intento de inserirgeolocalização aos registros de acesso é equivocado, pois fere direitos fundamentais comoda privacidade e intimidade.Há questões operacionais e técnicas que impedem ocumprimento das determinações constantes do Substitutivo, mas igualmente mostram-sepresentes questões éticas e jurídicas que não podem ser desrespeitadas. **Neste** sentido,mostra-se necessária a **REJEIÇÃO do PROJETO ORIGINAL E DO SUBSTITUTIVO apresentado na CCDD** do **Senado Federal.**

Este resumo executivo foi elaborado pela equipe técnica do Instituto 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.

Contato institucional ……icd@cidadaniadigital.in
……(61) 99856-6925

Category

1. Conteúdo Restrito

Date

CONSELHO DIGITAL
contato@conselhodigital.org.br

08/09/2024
Date Created
22/12/2023