CONSELHO DIGITAL
contato@conselhodigital.org.br

PL 6960-2017 NT 20.04.2023

versão ajustada em 20.04.2023

Resumo Executivo

Image2 Image not found or type unknown **PL 6.960/2017** | CCJC

APROVAÇÃO DO PARECER DA CCTCI

AUTOR: DEP. CLEBER VERDE (PRB/MA)

RELATOR: AGUARDANDO DESIGNAÇÃO DE RELATOR

TRAMITAÇÃO: CCTI • CSPCCO • CCJC • PLENÁRIO

EMENTA: Inviolabilidade de dados em terminais e acesso pela autoridade policial.

SE O TEXTO SUBSTITUTIVO FOR APROVADO

- Reduzirá a segurança das comunicações eletrônicas privadas.
- Permitirá a violação sistêmica da intimidade e da privacidade de milhões de brasileiros que utilizam a internet.
- Não aumentará a eficiência das investigações criminais.

O PL 6960/2017 estabelece a inviolabilidade do sigilo dos dados armazenados em terminais. O substitutivo aprovado na CCTCI e na CSPCCO vai na mesma linha, mantendo essa proteção, apenas excluindo a alteração do conceito de terminal, por entender desnecessária.

Na CCJC, foi apresentado parecer que, apesar de manter a inviolabilidade dos dados, vai

além e ***(i)*** dispensa necessidade de autorização judicial para a autoridade policial ou membro do Ministério Público requisitar registros de conexão e de acesso a aplicações de internet (art.10, §1º); ***(ii)*** permite que a autoridade policial, em caso de flagrante de crimes definidos em lei como hediondos, de tráfico de drogas ou terrorismo, acesse, sem autorização judicial, os dados de registro e conteúdos de comunicação privada de dispositivo móvel (art.10, §5º); e ***(iii)*** prevê o fornecimento de chave criptográfica quando necessária para acessar os dados e conteúdos de comunicação privada, nos casos de investigação de crimes hediondos e emprego, pelas polícias judiciárias, de técnicas e ferramentas tecnológicas que atinjam esse fim art.10, § 6º).

Ainda que louvável a preocupação com a segurança pública, as alterações restringem excessivamente a esfera de privacidade e liberdade dos usuários brasileiros, colocando em risco os preceitos consagrados no Marco Civil da Internet (MCI) e na Lei Geral de Proteção de Dados (LGPD).

VIOLAÇÃO À INTIMIDADE E AO SIGILO DAS COMUNICAÇÕES

Ao eliminar a necessidade de autorização judicial para requisição de dados, registros e até do conteúdo de comunicações privadas, o substitutivo da CCJC desrespeita a Constituição Federal (CF), que assegura a **inviolabilidade da intimidade e vida privada** e o **sigilo das comunicações** (art. 5º, X e XII), que pode ser quebrado **somente mediante ordem judicial**, em **último caso**, para fins de investigação criminal ou instrução processual penal.

O texto também viola ***(i)*** o Código Civil (CC), que protege a vida privada, atribuindo ao magistrado o poder de adotar medidas para impedir a sua violação (art. 21) e ***(ii)*** o Marco Civil da Internet (MCI) e a Lei Geral de Proteção de Dados Pessoais (LGPD), que baseiam-se no respeito à privacidade; à liberdade de expressão, de informação, de comunicação e de opinião; e na inviolabilidade da intimidade e da vida privada.

Buscando preservar esses direitos fundamentais dos cidadãos brasileiros, o MCI prevê que os provedores só estarão obrigados a disponibilizar registros de conexão e de acesso a aplicações de maneira autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou terminal mediante ordem judicial.

O crivo judicial é essencial para garantir que pedidos de requisição de dados infundados não violem direitos constitucionalmente assegurados, sendo papel exclusivo do Poder Judiciário **sopesar princípios constitucionais,** mediante o **devido processo legal**. O texto do substitutivo da CCJC, na prática, delega essa atribuição a agentes privados, transformando provedores em verdadeiros tribunais privados.

DESNECESSIDADE

O ordenamento brasileiro já prevê **mecanismos tecnicamente seguros** e **juridicamente adequados** para provimento de dados de identificação do usuário após ordens judiciais. Além disso, como exceção à regra geral (necessidade de ordem judicial), ***(i)*** o MCI já possibilita o fornecimento de dados cadastrais às autoridades administrativas que detenham competência legal para a sua requisição (art. 10, §3º, do MCI); e ***(ii)*** em alguns casos específicos e excepcionais previstos na legislação, dada a seriedade dos tipos penais, o delegado de polícia ou membros do Ministério Público podem requerer o acesso a dados de identificação, independentemente de ordem judicial.

ENFRAQUECIMENTO DOS MECANISMOS DE SEGURANÇA

O fornecimento da chave criptográfica, conforme estabelecido no texto, expõe os usuários a **risco exagerado** e injustificado, violando a garantia de segurança e funcionalidade da rede, prevista no MCI.

É preciso considerar ainda que a legislação brasileira **estimula o uso de mecanismos de segurança**, como a LGPD (art. 46), que impõe aos agentes de tratamento a obrigação de adotar medidas para proteger os dados pessoais e acessos não autorizados. Na mesma linha, ***(i)*** o Decreto 8.771/2016, que regulamenta o MCI, prevê, entre as diretrizes sobre padrões de segurança, "o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes" (art. 13, IV); ***(ii)*** o Decreto 7.845/2012 estabelece que os meios eletrônicos de armazenamento devem utilizar recursos criptográficos adequados ao grau de sigilo (art. 31); e ***(iii)*** a Resolução nº 4.658/2018, do Banco Central, incentiva que as instituições financeiras usem criptografia.

Assim, a busca por "descriptografar" as informações **esvazia o sentido do uso da criptografia** e mecanismos de segurança em geral, pois não é possível enfraquecer a criptografia apenas para uma situação específica.

Também vai na direção contrária à experiência internacional, que tem recomendado o uso de criptografia como um importante mecanismo de segurança: ***(i)*** o relatório sobre criptografia da ONU[1] apontou que seu uso permite o exercício de direitos fundamentais e que os Estados devem apresentar evidências suficientes de que as vulnerabilidades propostas para fins de investigação são o menos invasivas possível, especialmente à luz de outras ferramentas de investigação disponíveis; e ***(ii)*** a Human Rights Watch já se manifestou afirmando que o enfraquecimento da criptografia **não impede a ocultação de informações**, já que os agentes criminosos podem usar outros meios para esconder seus

dados e, na prática, a proposta apenas sujeita os usuários a **vulnerabilidades e riscos**[2].

[1]https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement

[2] https://www.hrw.org/news/2017/06/26/perils-back-door-encryption-mandates

PL 6.960/2017 | CONCLUSÃO

FAVORÁVEL AO PARECER DA CCTCI

Tal como previsto na Constituição, a privacidade e intimidade dos cidadãos brasileiros é inviolável, salvo exceções pontuais. Por isso, o acesso aos dados e às comunicações deve estar condicionado à análise do Poder Judiciário, que têm competência para avaliar a necessidade e adequação de restrições a esses direitos para fins de persecução penal. A Internet deve continuar a ser uma rede aberta e tecnologicamente neutra, capaz de sustentar uma gama sempre crescente de serviços e aplicações.

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

Image1

cidadaniadigital.in

Image not found or type unknown

Category

1. Conteúdo Restrito

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