Internet Society
Capítulo Brasil

Nota Técnica do GT de Criptografia da ISOC Brasil ao PL 4939/2020

Autores

Bruno Marcolini

Luiza Dutra

Pedro Amaral

Pedro Silva Neto

Thobias Prado Moura

03 de outubro de 2025

Internet Society
Capítulo Brasil

Nota Técnica do GT de Criptografia da ISOC Brasil ao PL 4939/2020

Sumário Executivo: Este documento apresenta uma análise do Projeto de Lei 4939/2020, que visa modernizar a legislação sobre a obtenção de prova em matéria penal. A análise conclui que, embora o projeto de lei parta de uma premissa legítima, alguns mecanismos — notadamente a previsão de retenção de dados em massa (Art. 7º), a flexibilização do acesso a registros de conexão e tráfego (Art. 14) e a autorização para o uso de "sensores ou métodos ofensivos" (Art. 15) — impactam de forma severa e negativa os habilitadores essenciais para uma Internet segura e confiável. Esta nota traz recomendações para alinhar o PL às melhores práticas internacionais e ao ordenamento jurídico brasileiro, incluindo: i) a substituição do modelo de retenção de dados em massa pela preservação direcionada (*targeted preservation*), mais proporcional e eficaz; ii) a reafirmação da exigência de ordem judicial fundamentada como condição indispensável para o acesso a dados de conexão e tráfego, protegidos pelo sigilo constitucional; e iii) a proibição explícita do uso de *spyware* e ferramentas de intrusão remota (*government hacking*) em dispositivos digitais, direcionando a interceptação telemática para os limites técnicos dos provedores de serviços. Essas alterações garantem que a capacidade investigativa do Estado seja aprimorada sem trazer riscos à segurança, a direitos fundamentais, como privacidade, confidencialidade e presunção de inocência e à integridade da infraestrutura digital.

1. Breve retomada

O Projeto de Lei 4939/2020 surge em um cenário de inegável urgência e relevância. A transição de crimes patrimoniais de rua para fraudes e estelionatos digitais, exemplificada pelos recentes e sofisticados ataques ao sistema PIX, vem demonstrando uma clara necessidade de modernizar o ordenamento jurídico brasileiro para a produção de provas em ambiente digital. Nesse sentido, o legislador busca, legitimamente, equipar as autoridades de persecução penal com ferramentas adequadas para enfrentar os desafios impostos pela criminalidade na era da informação. Destacamos positivamente a atenção especial dedicada a dados sensíveis e íntimos (Art. 26) e a exigência de participação de perito oficial para a implementação dos meios de obtenção da prova digital (Art. 22).

Contudo, a busca por eficácia investigativa, da forma como delineada em alguns dispositivos do PL, gera um paradoxo de segurança, ao se propor mecanismos que fragilizam a segurança de sistemas, a confidencialidade das comunicações e a privacidade dos cidadãos para facilitar investigações. Dessa forma, o projeto de lei pode, na prática, aumentar a superfície de ataque para os mesmos criminosos e agentes hostis que visa combater. Esta dinâmica impõe riscos consideráveis e inaceitáveis à soberania nacional, à ordem econômica e à segurança de todos os brasileiros.

Portanto, as propostas contidas nos artigos 14 e 15 do projeto de lei representam ameaças diretas e severas à privacidade, à confidencialidade e à confiabilidade dos sistemas, não afetando apenas os direitos individuais, mas comprometendo a saúde e a segurança de todo o ecossistema digital brasileiro. A seguir, cada um desses mecanismos será analisado em detalhe.

2. Análise dos Mecanismos do PL 4939/2020 e seus Impactos

Diante da transição de crimes patrimoniais para o ambiente digital, exemplificada por fraudes e ataques ao sistema PIX, a modernização da legislação para produção de provas se mostra inegável. O Projeto de Lei 4939/2020 busca responder a esse desafio e apresenta salvaguardas importantes.

Nesse sentido, destacam-se positivamente como pontos fortes do Projeto:

1. A atenção especial aos dados sensíveis e íntimos no contexto de investigações.
2. A obrigação de participação de perito oficial ou assistente técnico para implementação dos meios de obtenção da prova digital, no artigo 22.
3. A obrigação de registro e armazenamento dos atos eletrônicos praticados durante a operação e seu envio ao juiz e ao Ministério Público, no artigo 30.

É nesse contexto de combate ao crime digital, porém, que o PL gera um paradoxo de segurança. Ao propor mecanismos que fragilizam a confidencialidade e a segurança de sistemas para facilitar investigações, o texto pode, na prática, aumentar a insegurança cibernética e a vulnerabilidade aos mesmos agentes hostis

que visa combater, impondo riscos consideráveis à soberania, à ordem econômica e à segurança de todos os brasileiros.

2.1. Acesso a Dados (Art. 14)

O Artigo 14 da nova minuta do projeto de lei representa o retrocesso mais grave em relação à legislação vigente, ao autorizar expressamente o acesso a dados de comunicação sem a necessidade de autorização judicial prévia.

Os incisos I e II do Art. 14 estabelecem como meios de obtenção da prova digital, respectivamente, "A preservação imediata de informações de assinante, dados de conteúdo e de tráfego" e "A revelação imediata e parcial de dados de tráfego", ambos por requisição da autoridade legitimada e "independentemente de ordem judicial".

O acesso a registros de conexão, tráfego e conteúdo sem o escrutínio de um juiz representa uma violação direta e frontal do direito à privacidade e ao sigilo das comunicações, garantido pelo Art. 5º, XII, da Constituição Federal. Esses dados revelam com quem uma pessoa se comunica, quais sites visita, sua localização e seus padrões de comportamento, compondo um retrato íntimo de sua vida.

Além disso, cabe ressaltar ainda que a exigência de ordem judicial é um pilar do sistema de freios e contrapesos. Ela garante que a atividade investigativa do Estado seja supervisionada por um poder independente, prevenindo abusos e garantindo que a quebra de sigilo seja uma medida excepcional e justificada. Eliminar essa exigência para dados tão sensíveis destrói a *accountability* estatal e abre as portas para a vigilância arbitrária e em massa.

Por outro lado, é válido lembrar que o Marco Civil da Internet (MCI) diferencia dados cadastrais (nome, e-mail, profissão, endereço) dos registros de conexão e de acesso a aplicações de internet (o conjunto de informações referentes à data e hora de início e término de uma conexão, sua duração e o endereço IP utilizado).

Enquanto o Art. 10, § 3º, do MCI permite que autoridades administrativas requisitem dados cadastrais, o § 1º do mesmo artigo é inequívoco ao determinar que a disponibilização dos registros de conexão e de acesso a aplicações depende

de "prévia ordem judicial". Essa distinção não é arbitrária. Dados cadastrais identificam uma pessoa, mas os registros de conexão e acesso revelam suas atividades e comunicações, sendo, portanto, protegidos por maior grau de sigilo.

A proposta do Art. 14 do PL 4939/2020 permite que um conjunto muito mais amplo de dados (tráfego e até mesmo conteúdo) sejam acessados sem ordem judicial, o que representa um retrocesso legislativo sem precedentes[1]. Ressalta-se que a jurisprudência dos tribunais superiores brasileiros têm consistentemente reforçado a interpretação do MCI, e a própria Advocacia-Geral da União (AGU) já defendeu perante o Supremo Tribunal Federal (STF) a constitucionalidade da exigência de autorização judicial para o acesso a registros de conexão, argumentando que tais informações "interferem na intimidade e na privacidade do indivíduo".

No mais, o Art. 14 abre margem para a prática corriqueira de acesso a celulares durante abordagens policiais, muitas vezes realizadas de forma arbitrária e violenta contra pessoas negras e periféricas. Tal realidade conecta-se ao conceito conhecido como “criptoanálise de mangueira de borracha”: ação de agentes estatais no sentido de recorrer à coerção, física ou psicológica, para forçar indivíduos a desbloquearem seus dispositivos e acessarem dados criptografados. No Brasil, essa prática informal é frequentemente normalizada nos chamados “enquadros” e “baculejos”, aprofundando desigualdades raciais e sociais.

Portanto, a redação do Art. 14 é uma ameaça direta à segurança jurídica, colocando cidadãos e provedores de serviços em uma posição de extrema vulnerabilidade. Ela cria um ambiente onde a vigilância pode se tornar a regra, e não a exceção, minando a confiança fundamental necessária para o funcionamento da economia digital e o exercício de liberdades online.

---

[1] Uma coleta ampla da forma como está descrita impacta diretamente a arquitetura de confiança da Internet. A previsibilidade de que o sigilo de dados sensíveis de conexão e tráfego só pode ser quebrado mediante ordem judicial fundamentada é um pilar para o exercício de liberdades online e para a segurança de transações na economia digital. A flexibilização dessa garantia gera um efeito inibidor (*chilling effect*) sobre a livre expressão e a participação social, além de minar a confiança de usuários e empresas em serviços digitais, comprometendo o ambiente de inovação e a saúde de todo o ecossistema digital brasileiro.

2.2. Interceptação Telemática (Art. 15)

O Artigo 15 contém o conceito mais problemático do PL: a autorização para o uso de "sensores ou ferramentas de vigilância" para acessar dados, legalizando na prática o *hacking* governamental. O § 1º do Art. 15 autoriza que a interceptação telemática seja efetuada "através da inserção de sensor informático ou ferramenta de vigilância em um sistema de tecnologia da informação e da comunicação".

Hacking governamental consiste em explorar vulnerabilidades não intencionais, criando um estoque de vulnerabilidades e incentivo para não corrigi-las, tornando o ambiente digital mais inseguro para todos. O ciberataque global WannaCry, por exemplo, que em 2017 paralisou sistemas de saúde e empresas em todo o mundo, é o exemplo mais emblemático desse risco. Ele foi possibilitado justamente pela exploração de uma vulnerabilidade de software que havia sido descoberta e acumulada por uma agência de inteligência estatal estadunidense, e que posteriormente vazou. Backdoors, por sua vez, consistem em criar uma vulnerabilidade intencional no design de um produto. No entanto, é tecnicamente inviável que tais vulnerabilidades sejam usadas apenas por agentes 'autorizados'.

Tecnicamente "a inserção de sensor informático ou ferramenta de vigilância" parece se referir à implantação de softwares maliciosos (*malware* ou *spyware*) que exploram vulnerabilidades em sistemas ou aplicativos para obter acesso a dispositivos. Essa prática é fundamentalmente diferente de uma interceptação telemática tradicional, que ocorre nos servidores de um provedor de serviços.

A criptografia ponta-a-ponta é o padrão ouro de segurança e privacidade digitais. Ela é a principal garantia para que as informações e comunicações sejam protegidas contra acessos não autorizados por agentes maliciosos. Sem sua difusão massiva, os cidadãos brasileiros e de todo o mundo estariam muito mais vulneráveis a violações do sigilo de suas comunicações e informações e, consequentemente, de golpes, fraudes e outras formas de crimes digitais.

Nesse debate, o *hacking* governamental é por vezes apresentado como uma alternativa a propostas de enfraquecimento da criptografia, como a criação de *backdoors* (portas dos fundos). No entanto, ambas as abordagens são extremamente danosas para a segurança digital. A tabela abaixo compara as

diferentes abordagens para o acesso a dados criptografados, evidenciando os riscos sistêmicos das opções que o PL 4939 implicitamente autoriza.

Abordagem	Descrição Técnica	Impacto na Segurança Sistêmica	Implicações para Direitos Fundamentais
Backdoors na Criptografia	Inserção de falhas deliberadas no código de produtos e serviços para permitir acesso governamental.	Catastrófico. Enfraquece a segurança para todos os usuários, tornando-os vulneráveis a qualquer ator (criminoso, estatal, etc.) que encontre e explore a falha deliberada.	Violação da privacidade em massa, erosão da confiança e da confidencialidade das comunicações.
Hacking Governamental (Métodos Ofensivos)	Exploração de vulnerabilidades de software existentes (não intencionais) para invadir dispositivos de alvos específicos.	Muito Alto. Incentiva o acúmulo de vulnerabilidades em vez de sua correção, deixando todo o ecossistema digital inseguro e vulnerável a ataques por terceiros.	Violação profunda da privacidade do alvo e de seus contatos; alto risco de danos colaterais e acesso a dados além do escopo da autorização judicial.
Cooperação Legal e Preservação Direcionada	Uso de canais legais (como ordens judiciais e tratados de cooperação internacional - MLATs) para solicitar dados a provedores, respeitando a jurisdição e o devido processo legal.	Nulo ou Positivo. Fortalece a cooperação, o Estado de Direito e a segurança jurídica sem criar novas vulnerabilidades técnicas na infraestrutura da Internet.	Respeita o devido processo legal, a privacidade e a soberania, com a quebra de sigilo sendo uma medida excepcional e controlada pelo Judiciário.

A análise comparativa demonstra que a abordagem mais segura e respeitosa aos direitos é a que se baseia na cooperação legal, e não na criação ou exploração de falhas técnicas.

2.3. Retenção e Acesso a Dados de Assinantes (Art. 7º)

A nova redação do Artigo 7º abandona a controversa retenção de dados em massa da versão anterior, mas introduz uma nova preocupação: a requisição direta de dados cadastrais detalhados sem ordem judicial. O Art. 7º, § 1º, permite que a autoridade policial ou o Ministério Público requisitem diretamente aos provedores, "independentemente de ordem judicial", informações como nome, endereço, dados de contato, informações de pagamento e até a localização de instalação de equipamentos de comunicação.

A nova redação do Art. 7º parece tentar se alinhar com a distinção do Marco Civil da Internet, permitindo o acesso direto a dados cadastrais. No entanto, a definição de "Informações sobre assinantes" no Art. 3º é extremamente ampla, incluindo dados que vão além da simples qualificação. O acesso a informações de pagamento e, principalmente, à "localização de instalação do equipamento de comunicação" sem ordem judicial é problemático e pode ser desproporcional.

Além disso, a ausência de mecanismos claros de auditoria e de controle externo compromete a rastreabilidade do acesso e a delimitação temporal da utilização dos dados pelas autoridades. A omissão quanto ao tratamento de conteúdos protegidos por criptografia agrava o quadro, permitindo interpretações que podem fragilizar a segurança dos sistemas[2]. Na prática, a combinação desses fatores resulta na criação de um regime de vigilância indiscriminada, semelhante ao modelo de d*ata retention*.

A alternativa superior continua sendo o modelo de preservação direcionada (*targeted preservation*), onde, mediante ordem judicial, dados específicos de um investigado são preservados. Este método, alinhado a instrumentos como a

[2] Algumas questões centrais precisam ser melhor esclarecidas. Como será monitorado o acesso? Por quanto tempo as autoridades poderão armazenar esses dados? E como ficam os conteúdos protegidos por criptografia, que o texto sequer menciona?

Convenção de Budapeste, é mais eficaz e respeita o princípio da minimização de dados da LGPD.

2.4. Técnicas Especiais de Investigação (Arts. 28-30)

Em um ponto positivo, a nova versão do projeto de lei aprimora as salvaguardas para técnicas especiais de investigação, contudo, a redação do artigo 28º, que autoriza a infiltração virtual de agentes em redes de dados gera uma série de riscos. A previsão de identidades fictícias, com possibilidade de operação por até 360 dias, cria margem para práticas de vigilância preventiva, criminalização de movimentos sociais e até mesmo operações encobertas em massa. Ainda que prevista a necessidade de autorização judicial, o regime proposto confere poderes desproporcionais e carece de mecanismos de transparência e prestação de contas.

Com relação ao Artigo 30 da nova minuta, o mesmo determina que, concluída a investigação, "todos os atos eletrônicos praticados durante a operação deverão ser registrados e armazenados, devendo ser encaminhados ao juiz e ao Ministério Público, juntamente com relatório circunstanciado".

Assim, a exigência de registro integral dos atos eletrônicos é essencial e positiva para estabelecer uma cadeia de custódia digital robusta e confiável, uma vez que o registro detalhado é a única maneira de garantir que a prova foi obtida legalmente e não foi adulterada, permitindo que a defesa exerça seu direito de auditar os procedimentos e que o Judiciário possa avaliar a validade da prova. A transparência processual não é um obstáculo à eficácia investigativa; pelo contrário, é uma condição indispensável para sua legitimidade no Estado Democrático de Direito.

3. RECOMENDAÇÕES

Por fim, com base na análise de impacto detalhada na seção anterior, esta seção consolida e fundamenta as propostas de alteração ao PL 4939/2020 (versão 2025). Cada recomendação é apresentada como uma solução direta para os riscos identificados. Se propõe as seguintes alterações para reduzir riscos à segurança:

1. Adaptação da retenção de dados para harmonizar com a inviolabilidade das comunicações, a minimização da coleta de dados e o Marco Civil da Internet.
2. Especificar a previsão de interceptação telemática para remover margem a soluções que ameaçam gravemente direitos e segurança dos sistemas digitais.
3. Reduzir riscos às liberdades pela infiltração virtual e ações disfarçadas.
4. Redução do tempo e exceções para manutenção de dados sensíveis e íntimos.
5. Adoção de salvaguardas de equivalência de proteção de dados pessoais para compartilhamento internacional de dados

3.1. Princípios e Fundamentos da Lei

Proposta de redação:

"Artigo 2º - Esta Lei será pautada pelos seguintes princípios e fundamentos:

(...)

VII – Transparência, interpretabilidade e explicabilidade dos meios de obtenção da prova digital e das operações com os dados das investigações.

Y - o Direito Fundamental à Proteção de Dados Pessoais e os princípios da necessidade, proporcionalidade, qualidade, segurança e prevenção.
X - a integridade e a confiabilidade dos sistemas informáticos e dos dados;"

3.2. Definições de Dados Cadastrais - Harmonização com a categoria do Marco Civil da Internet (MCI):

Proposta de redação:
"Art. 3º. Para efeitos desta Lei considera-se:
(...)
VI –
(...)
b) A qualificação pessoal do assinante, compreendida esta como os dados cadastrais dos serviços, incluindo nome, prenome, estado civil e profissão, bem como a filiação, endereço postal, virtual ou geográfico, dados para contato, ou

outro modo de acesso, e informações de cobrança ou pagamento, disponíveis com base no contrato ou acordo de serviço;"

3. 3. Retenção e Preservação de Dados (Art. 7º)

A redação atual estimula coleta massiva de dados, aumentando os ganhos de atacantes e a superfície de ataque. Confronta diretamente a minimização de dados prevista na LGPD, bem como os princípios de finalidade, necessidade e adequação. Amplia em demasia e de forma genérica a obrigação de retenção para categorias de dados, dispensando ordem judicial para o acesso a registros. Propomos o modelo de preservação direcionada, usado na própria Convenção de Budapeste.

Proposta de redação:

±Art. 7º Os fornecedores de serviços deverão manter registros estritamente necessários à operação técnica de suas atividades, pelo prazo máximo de 1 (um) ano, sendo vedada a coleta ou conservação de dados adicionais que não sejam indispensáveis à prestação do serviço.

§ 1º Dados de tráfego ou de conteúdo somente poderão ocorrer mediante ordem judicial fundamentada, observados os princípios da necessidade, adequação e proporcionalidade.

§ 2º Em casos de investigação de crimes graves, definidos em lei, e havendo risco iminente de perda da prova, a autoridade policial ou o Ministério Público poderão requisitar a preservação imediata dos dados, comunicando-a ao Poder Judiciário no prazo de 24 (vinte e quatro) horas para ratificação da medida.

§ 4º É vedada a retenção indiscriminada de dados de todos os usuários."

3.4. Acesso a Dados sem Ordem Judicial (Art. 14, I e II)

A redação atual conflita com a garantia constitucional da inviolabilidade das comunicações (art. 5º, XII, da CF).

Proposta de redação:

Art. 14 - Constituem meios de obtenção da prova digital:

I – a preservação imediata de informações de assinante, dados de conteúdo e de tráfego armazenados em um sistema de tecnologia da informação e da comunicação sob responsabilidade de fornecedor de serviços ou controlador de dados, desde que determinada por ordem judicial fundamentada, observado o prazo máximo de 60 (sessenta) dias, prorrogável uma única vez, mediante decisão igualmente fundamentada;

II – a revelação parcial de dados de tráfego, em quantidade estritamente suficiente para permitir a identificação de fornecedores de serviços e da rota da comunicação, exclusivamente mediante autorização judicial, podendo a autoridade policial ou o Ministério Público requerer a medida em caráter de urgência, com comunicação imediata ao juiz, que decidirá em até 24 (vinte e quatro) horas;

3.5. Interceptação Telemática (Art. 15)

O art. 15 regula a interceptação telemática e abre a possibilidade de o juiz autorizar "sensores ou métodos ofensivos" para acessar dados quando a criptografia impedir a colaboração do provedor. A redação pode facilitar o uso de *spyware*, ferramentas internacionalmente reconhecidas por danos à segurança cibernética e violações aos direitos fundamentais.

Proposta de redação:

Art. 15. A interceptação telemática poderá ser destinada aos fornecedores de serviços e controladores de dados de todas as naturezas, respeitando os limites de suas capacidades técnicas.

§ 1º. Presentes os requisitos de razoabilidade e proporcionalidade, também pode ser efetuada a interceptação telemática através da inserção de sensor informático ou ferramenta de vigilância em um sistema de tecnologia da informação e da comunicação, desde que não reduza a segurança dos dados, redes e sistemas.

§ 2º A interceptação telemática seguirá subsidiariamente o procedimento estabelecido para a interceptação telefônica, especialmente quanto ao prazo, à cadeia de custódia e à intimação dos interessados, quando cabível.

§ 3º A ordem judicial será dirigida exclusivamente a fornecedores de serviços e controladores de dados, vedada a utilização de softwares maliciosos e espiões, assim como de ferramentas de intrusão remota em dispositivos de usuários.

§ 4º A medida deverá respeitar o princípio da minimização de dados, restringindo-se ao estritamente necessário para a investigação.

6. Garantias ao Direito de Defesa e ao Sigilo Profissional

Art. 19. (...)

I - O uso de técnicas especiais de investigação digital deverá ser integralmente registrado em auto circunstanciado, garantindo transparência e possibilidade de auditoria pelas partes, sem prejuízo do sigilo sobre vulnerabilidades técnicas empregadas.

Art. 25. Os meios de obtenção da prova digital observarão o sigilo em razão de função, ministério, ofício ou profissão, incluindo, mas não se limitando, o sigilo médico, religioso, das fontes jornalísticas e o sigilo da relação advogado e cliente.