REVISTA
MATO GROSSENSE
DE DIREITO
ISSN: 2965-1050
REVISTA CIENTÍFICA REMAD - VOLUME 3 - NÚMERO 2 - NOVEMBRO DE 2025.

A QUEBRA DE SIGILO TELEMÁTICO: análise jurisprudencial, doutrinária e legal

YASMIN CAROLINE DA COSTA CARVALHO[1]
MARIANA CAROLINA DELUQUE ROCHA[2]

RESUMO: As quebras de sigilo telemático no processo penal brasileiro têm se tornado instrumentos centrais nas investigações criminais contemporâneas, especialmente diante da ampla utilização de dispositivos móveis e da internet. A Constituição Federal, em seu artigo 5º, inciso XII, assegura o sigilo das comunicações, permitindo sua quebra apenas por decisão judicial devidamente fundamentada. Leis como a nº 9.296/1996 e a nº 12.965/2014 (Marco Civil da Internet) regulam o acesso a dados e comunicações armazenadas, mas ainda apresentam lacunas frente à complexidade das provas digitais. A ausência de regulamentação específica provoca insegurança jurídica e decisões conflitantes no âmbito judicial. Com foco nas decisões jurisprudências, o estudo examina como os tribunais têm aplicado essas normas e quais os limites constitucionais para a obtenção de dados digitais. A pesquisa, fundamentada em revisão bibliográfica e análise jurisprudencial, evidencia a urgência de atualização normativa e de uniformização da jurisprudência para garantir a legalidade e a proteção aos direitos fundamentais.
Palavras-chave: Prova digital; Sigilo telemático; Marco Civil da Internet; Interceptação.

THE TELECOMMUNICATIONS SECRECY BREACH: jurisprudential, doctrinal and legal analysis

ABSTRACT: Telematic secrecy breaches in Brazilian criminal proceedings have become central instruments in contemporary criminal investigations, especially given the widespread use of mobile devices and the internet. The Federal Constitution, in its article 5, item XII, ensures the secrecy of communications, allowing their breach only by a duly substantiated judicial decision. Laws such as No. 9,296/1996 and No. 12,965/2014 (Marco Civil da Internet) regulate access to stored data and communications, but still present gaps in the face of the complexity of digital evidence. The lack of specific regulation causes legal uncertainty and conflicting decisions in the judicial sphere. Focusing on case law decisions, the study examines how the courts have applied these rules and what the constitutional limits are for obtaining digital data. The research, based on a bibliographic review and case law analysis, highlights the urgency of updating regulations and standardizing case law to ensure legality and the protection of fundamental rights.
Keywords: Digital evidence; Telematic secrecy; Internet Civil Rights Framework; Interception.

[1] Acadêmica de Direito, Faculdade Fasipe Cuiabá. Endereço eletrônico: yasmin.carolinemaria@gmail.com
[2] Professora Mestra em Direito. Faculdade Fasipe Cuiabá. Endereço eletrônico:advmarianadeluque@gmail.com.

1 INTRODUÇÃO

O desenvolvimento tecnológico transformou profundamente a interação entre o mundo e a sociedade. Desde o século XX, na sociedade da informação, a tecnologia passou a integrar todos os aspectos da vida humana.

A década de 1980 marcou o avanço com o uso e a popularização dos computadores, a expansão da internet e, posteriormente, a disseminação de smartphones e notebooks.

Essa evolução modificou as formas de comunicação e de armazenamento de dados, possibilitando a coleta massiva de informações e ampliando a vigilância sobre as atividades humanas.

No campo jurídico, o direito penal passou a utilizar os avanços tecnológicos em investigações e na obtenção de provas, colocando a tecnologia e a internet no centro das discussões sobre o sistema penal contemporâneo.

Contudo, o Brasil ainda avança de forma restrita na regulamentação das provas digitais e dos métodos de coleta de evidências, especialmente quanto ao uso da internet e das comunicações digitais.

A Constituição Federal, em seu artigo 5º, inciso XII, garante a inviolabilidade das comunicações e do sigilo de dados, permitindo sua quebra apenas por ordem judicial e para fins de investigação criminal ou instrução processual penal.

Nesse contexto, a Lei nº 9.296/1996 regulamentou as interceptações telefônicas e telemáticas, e o Marco Civil da Internet (Lei nº 12.965/2014) estabeleceu princípios e garantias para o uso da internet, determinando que o compartilhamento de dados só ocorra mediante ordem judicial.

Apesar dos avanços, ainda há insuficiência normativa sobre provas digitais. O artigo 240 do Código de Processo Penal, que trata da busca e apreensão de objetos físicos, vem sendo aplicado de forma adaptada para justificar o acesso a dados digitais, embora seja inadequado para lidar com a complexidade dessas situações.

Essa lacuna legal gera instabilidade jurídica e pode levar a abusos, comprometendo os direitos fundamentais à privacidade e ao sigilo das comunicações.

Por isso, é essencial definir os limites das quebras de sigilo telemático e o papel do Judiciário na fixação de parâmetros. Embora não haja norma específica sobre busca e apreensão de dados digitais, os tribunais reconhecem que o artigo 240 do Código de Processo Penal não é suficiente.

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) reforçou a importância da inviolabilidade dos dados pessoais e do tratamento adequado das informações, inclusive na esfera penal.

Distingue-se a quebra de sigilo telemático da quebra de sigilo telefônico, pois, embora semelhantes, envolvem naturezas diferentes de comunicação e exigem regulamentações próprias.

As comunicações em tempo real têm caráter efêmero e direto, enquanto as armazenadas podem ser acessadas posteriormente, demandando níveis distintos de proteção.

Por fim, o objetivo central é analisar as quebras de sigilo envolvendo comunicações telemáticas, diferenciando as comunicações em tempo real das armazenadas, e ressaltando a importância de critérios claros e proporcionais.

2 REVISÃO DE LITERATURA

2.1 Quebra de Sigilo Telemático

A quebra de sigilo telemático, segundo Doneda (2015), é uma medida judicial que autoriza o acesso a dados armazenados em meios eletrônicos, como redes sociais, e-mails, serviços de nuvem e dispositivos físicos (smartphones e computadores).

Trata-se de importante instrumento de investigação, mas que deve respeitar os limites constitucionais e legais.

Constitucionalmente, o artigo 5º, XII, da Constituição Federal assegura a inviolabilidade das comunicações e dos dados, permitindo sua restrição apenas por ordem judicial, nas hipóteses previstas em lei e com finalidade de investigação criminal ou instrução processual.

No plano infraconstitucional, o artigo 10, §2º, do Marco Civil da Internet (Lei nº 12.965/2014) reforça esse entendimento ao exigir autorização judicial para o acesso ao conteúdo de comunicações privadas.

Assim, observa-se que o legislador buscou reforçar o caráter excepcional da medida, condicionando-a ao controle jurisdicional prévio, de forma a compatibilizá-la com as garantias fundamentais do ordenamento jurídico.

Doneda (2015) destaca que a medida não se limita a mensagens eletrônicas, abrangendo também listas de contatos, registros de localização, histórico de navegação e arquivos digitais, informações que permitem identificar hábitos e comportamentos, exigindo, portanto, proteção reforçada à luz dos direitos fundamentais à intimidade e à privacidade.

Como observam Vieira e Santos (2025), a ausência de regulamentação específica gera insegurança jurídica e pode favorecer abusos na fiscalização estatal, comprometendo a proteção constitucional ao sigilo das comunicações.

Quanto aos dados armazenados em dispositivos físicos, sua apreensão deve seguir os artigos 240 e seguintes do Código de Processo Penal, que regulam a busca e apreensão e exigem decisão judicial fundamentada, delimitando o objeto da medida, em observância ao princípio da reserva de jurisdição.

Nesses casos, exige-se decisão judicial previamente fundamentada, contendo a delimitação precisa do objeto da medida, em conformidade com o princípio da reserva de jurisdição e com as garantias do devido processo legal.

Por fim, Doneda (2015) adverte que, embora essencial à investigação criminal moderna, a quebra de sigilo telemático deve ser aplicada com cautela e proporcionalidade, equilibrando a eficiência da persecução penal com a proteção dos direitos fundamentais, em respeito aos valores do Estado Democrático de Direito.

2.1.1 Inviolabilidade do sigilo

O artigo 5º, inciso XII, da Constituição Federal de 1988 garante a inviolabilidade do sigilo das comunicações, assegurando a privacidade e a liberdade individual. Contudo, admite-se a quebra do sigilo telefônico mediante autorização judicial, apenas para fins de investigação criminal ou instrução processual penal.

Com o avanço da tecnologia, surgiram novos meios de comunicação (como a internet), o que tornou necessária uma reinterpretação do texto constitucional, originalmente pensado para comunicações telefônicas.

Autores como Alves (2023) e Sidi (2016) destacam que o Brasil ainda carece de regulamentação adequada sobre provas digitais e coleta de evidências eletrônicas.

Tomasevicius Filho (2016) reforça que o acesso a dados e registros de usuários deve depender de ordem judicial, e Barbosa (2020) observa que a simples aplicação do artigo 240 do Código de Processo Penal não é suficiente diante da complexidade das informações digitais.

No debate doutrinário promovido pelo InternetLab, estudiosos como Ferraz Jr. (2018), Sidi (2016) e Quito (2022) discutiram a dificuldade de separar “fluxo” e “resultado” das comunicações no ambiente digital, já que no mundo virtual o armazenamento faz parte do próprio processo comunicativo.

Além disso, os doutrinadores analisam o texto normativo do artigo 5º, XII, da Constituição Federal, afirmando que o objeto de proteção constitucional é a liberdade de pensamento, isto é, a liberdade que tem cada indivíduo de se expressar sem receio de que seu pensamento venha a ser conhecido por um terceiro estranho à comunicação.

A falta de clareza constitucional quanto às exceções ao sigilo levou à discussão sobre a Lei nº 9.296/1996, que regula a interceptação telefônica.

O parágrafo único do artigo 1º estendeu essa disciplina às comunicações telemáticas e informáticas, o que gerou controvérsia sobre possível excesso normativo, já que a Constituição menciona expressamente apenas as comunicações telefônicas.

Em síntese, o debate gira em torno da interpretação e ampliação do sigilo constitucional diante das novas tecnologias, buscando equilibrar a proteção da privacidade e a efetividade das investigações criminais.

2.1.2 Características e espécies jurídicas

A palavra telemática resulta da junção de informática e telecomunicação, representando a integração entre tecnologias computacionais e sistemas de transmissão de dados.

Segundo Velloso (2014), o avanço tecnológico da década de 1980, marcado pela popularização dos computadores e expansão da internet, possibilitou a consolidação da chamada Era da Informação, caracterizada pela comunicação digital em larga escala.

Para Sidi (2016), a comunicação é considerada telemática quando ocorre de forma digital, por meio da conversão de informações em séries binárias, abrangendo transmissões via internet e outros meios eletrônicos.

Nesse contexto, a telemática tornou possível a comunicação entre máquinas e a circulação de dados em redes globais (Rossini, 2004).

Conforme Vaz (2012), essa evolução digital transformou documentos, músicas, imagens e comunicações tradicionais em formatos eletrônicos, alterando profundamente o modo como a sociedade se comunica e armazena informações.

A quebra de sigilo telemático, por sua vez, tem natureza cautelar, pois deve ser executada sob sigilo até sua efetivação, garantindo a eficácia da medida (Badaró, 2017).

Essa medida pode alcançar comunicações em curso, conteúdos armazenados, metadados e dados cadastrais, desde que autorizada judicialmente, conforme o artigo 5º, incisos X e XII, da Constituição Federal, que asseguram a inviolabilidade da intimidade e do sigilo das comunicações.

Contudo, a ausência de definições legais precisas gera confusão terminológica quanto ao uso do termo “quebra de sigilo telemático”, que abrange diferentes tipos de acesso a dados e comunicações.

Ainda assim, trata-se sempre de um meio de obtenção de prova, utilizado para coletar elementos relevantes à investigação criminal (Badaró, 2017).

A legislação processual brasileira disciplina poucos desses meios no Código de Processo Penal, sendo a busca e apreensão (arts. 240 a 250) o único regulado de forma expressa. Outros, como as interceptações telemáticas, quebras de sigilo bancário e fiscal e infiltração de agentes, encontram previsão em leis especiais.

Ademais, com o Pacote Anticrime (Lei nº 13.964/2019), o legislador inovou ao criminalizar a captação ambiental sem autorização judicial, incluindo o artigo 10-A na Lei nº 9.296/1996, reforçando a necessidade de controle judicial e respeito às garantias constitucionais na obtenção de provas digitais.

2.1.2.1 Interceptações telemáticas

Por interceptação, entende-se a intrusão de terceiros não autorizados no fluxo de comunicações privadas enquanto estas ocorrem. Conforme Greco (2020), trata-se da captação da conversa por terceiro, com ou sem o conhecimento dos interlocutores.

Esta prática suscita relevantes discussões sobre privacidade e legalidade das intervenções nas comunicações pessoais.De acordo com Vaz (2012), a interceptação consiste na captação de dados em trânsito por redes eletrônicas, podendo abranger correio eletrônico, comunicações via IP ou serviços de mensagens instantâneas.

O artigo 1º, parágrafo único, da Lei nº 9.296/1996 estende às comunicações telemáticas o mesmo regime jurídico das interceptações telefônicas, exigindo ordem judicial e segredo de justiça.

Sidi (2016) define a interceptação telemática como meio cautelar de obtenção de prova, cujo material é usualmente armazenado em mídias digitais.

Khedi (2008) destaca duas correntes doutrinárias sobre o alcance do artigo 5º, XII, da Constituição: a primeira sustenta a inviolabilidade absoluta das comunicações de dados, enquanto a segunda admite sua interceptação sob o mesmo regime das comunicações telefônicas, posição que prevaleceu na doutrina e na jurisprudência.

A Lei nº 9.296/1996 estabelece que a medida somente pode ser deferida quando houver indícios razoáveis de autoria, imprescindibilidade do meio e infração punida com reclusão. Barroso (2019) complementa que a análise deve observar o princípio da proporcionalidade em suas três dimensões: adequação, necessidade e proporcionalidade em sentido estrito.Embora o diploma legal discipline a interceptação telefônica, a ausência de detalhamento sobre a execução da interceptação telemática demanda interpretação judicial e adaptação técnica, sobretudo diante de novas modalidades de comunicação digital.

2.1.2.2 Comunicações telemáticas armazenadas

Segundo Rapôso (2019), a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) foi criada para garantir os direitos fundamentais à liberdade, privacidade e livre desenvolvimento da personalidade, regulando o tratamento de dados pessoais em formatos físico e digital, por pessoas físicas ou jurídicas, públicas ou privadas.

Contudo, a Lei nº 9.296/1996, que trata das interceptações de comunicações, não prevê expressamente o acesso a comunicações telemáticas armazenadas. Mesmo assim, a liberação de mensagens pretéritas tem sido autorizada judicialmente em investigações criminais, ainda que envolva controvérsias constitucionais e ausência de critérios legais claros.

De acordo com Abreu e Antonialli (2018), existem dois regimes jurídicos aplicáveis: (i) quando o acesso se dá por meio de provedores, aplica-se o Marco Civil da Internet (art. 7º, III), que exige ordem judicial, mas sem critérios específicos; e (ii) quando ocorre

diretamente em dispositivos apreendidos, aplica-se o artigo 240 do Código de Processo Penal, referente à busca e apreensão.

Portanto, embora o acesso a comunicações armazenadas também represente uma restrição a direitos fundamentais, a prática investigativa nem sempre observa os critérios de proporcionalidade e necessidade, o que evidencia a urgência de uma regulamentação específica e equilibrada para esse tipo de medida.

2.1.2.3 Coleta de dados

A quebra de sigilo telemático envolve o acesso a dados armazenados em dispositivos eletrônicos ou servidores, como mensagens, contatos, registros de localização, histórico de navegação e arquivos diversos. Essas informações podem estar tanto nos equipamentos dos investigados quanto em servidores de provedores de internet.

A legislação brasileira não dispõe de norma específica sobre o tema, havendo apenas o artigo 13-B do Código de Processo Penal, que autoriza o acesso, mediante ordem judicial, a dados de localização em casos de tráfico de pessoas. O dispositivo, contudo, é criticado por restringir o direito à intimidade e à vida privada assegurado no artigo 5º, inciso X, da Constituição Federal.

Na prática, as autoridades recorrem aos artigos 240 e seguintes do Código de Processo Penal, relativos à busca e apreensão, para justificar o acesso a dados telemáticos. Conforme Lopes Jr. (2019), tais medidas devem ser judicialmente autorizadas, com mandado preciso e fundamentado, indicando local e objeto da busca.

Em relação aos dados armazenados em servidores, o Judiciário tem aplicado o mesmo fundamento legal, tratando-os como documentos passíveis de apreensão remota (Quito, 2022). Contudo, a falta de regulamentação própria faz com que o acesso dependa apenas de ordem judicial, sem critérios quanto à finalidade ou à temporalidade da coleta.

Por fim, como observa Alves (2023), os smartphones funcionam hoje como extensões da vida pessoal, abrigando dados sensíveis que revelam hábitos e comportamentos. Assim, a quebra de sigilo dessas informações, ainda que para fins investigativos, pode representar grave violação à privacidade, exigindo limites legais claros e proporcionais.

2.1.2.4 Metadados

Os metadados são registros gerados pelo uso de aplicações na internet como data, hora, localização e endereço IP e são regulamentados pelo Marco Civil da Internet (Lei nº 12.965/2014). Segundo Abreu e Antonialli (2018), eles compreendem informações sobre comunicações, como remetente, destinatário e localização, mas não o conteúdo da mensagem. A Anatel (2020) explica que o IMEI é um exemplo de dado identificador de aparelhos móveis. Já Sidi (2016) amplia o conceito ao incluir dados de tráfego e duração das comunicações.

Esses registros de conexão devem respeitar a intimidade e a vida privada, conforme o artigo 10 do Marco Civil da Internet (Lei nº 12.965/2014), e só podem ser acessados mediante autorização judicial, salvo em casos de dados cadastrais básicos.

O artigo 22 da mesma lei estabelece os requisitos para o acesso judicial a tais registros: indícios do ilícito, justificativa da utilidade dos dados e delimitação temporal.

Estas exigências visam garantir a proporcionalidade e a necessidade da medida, equilibrando o poder investigativo com a proteção de direitos fundamentais.

No contexto recente, o Supremo Tribunal Federal (Rcl 75093 AgR-ED, Rel. Min. André Mendonça, 2025) reconheceu a legitimidade do acesso a metadados extraídos de aparelhos apreendidos, desde que voltado à obtenção de provas digitais já produzidas.

Assim, conforme Gonçalves (2022), a quebra de sigilo de metadados é uma medida legítima e indispensável à investigação, desde que não invada o conteúdo protegido das comunicações.

2.1.2.5 Dados cadastrais

O artigo 10 do Marco Civil da Internet (Lei nº 12.965/2014) estabelece que o acesso a dados cadastrais, registros de conexão e de acesso a aplicações deve observar a garantia constitucional à intimidade e à vida privada (art. 5º, X, CF).

O Decreto nº 8.771/2016 complementa essa norma ao definir, em seu artigo 11, § 2º, quais informações configuram dados cadastrais, filiação, endereço e qualificação pessoal, e determina que provedores sem tais dados não estão obrigados a fornecê-los, desde que comuniquem formalmente essa condição.

O § 3º do artigo 10 da mesma lei permite excepcionalmente o acesso a dados cadastrais por autoridades administrativas com competência legal, desde que o pedido seja motivado e fundamentado, conforme reforça o artigo 11 do Decreto nº 8.771/2016.

Esta exigência busca assegurar transparência e respeito aos direitos fundamentais à privacidade e à proteção de dados pessoais.

Segundo Quito (2022), a reserva de jurisdição deve prevalecer como regra geral, sendo o acesso direto admitido apenas em hipóteses expressamente previstas em lei.

Essas exceções estão dispostas no artigo 17-B da Lei nº 9.613/1998 (lavagem de dinheiro), no artigo 15 da Lei nº 12.850/2013 (organizações criminosas) e nos artigos 13-A e 13-B do Código de Processo Penal, que tratam de crimes graves como sequestro, tráfico de pessoas e extorsão mediante sequestro.

Por se tratarem de exceções à regra da reserva judicial, tais dispositivos devem ser interpretados restritivamente, limitando o acesso direto a dados cadastrais apenas aos crimes expressamente previstos.

Como destacam Abreu e Antonialli (2018), essas normas resultam de pressões das autoridades investigativas por maior agilidade, sob o argumento de que dados cadastrais não estariam protegidos pelo artigo 5º, X ou XII, da Constituição, o que, contudo, exige cautela diante da necessidade de preservar os direitos fundamentais à privacidade e à inviolabilidade dos dados pessoais.

2.1.2.6 Quebra de sigilo telemático e quebra de sigilo telefônico

A quebra de sigilo telemático e a quebra de sigilo telefônico são medidas investigativas excepcionais, ambas amparadas pelo artigo 5º, XII, da Constituição Federal, que admite o afastamento do sigilo das comunicações apenas mediante ordem judicial fundamentada e nos casos previstos em lei.

O sigilo telemático refere-se ao acesso a dados e comunicações eletrônicas (como e-mails, mensagens em aplicativos, registros de navegação e informações armazenadas em servidores), sendo regulamentada principalmente pelo Marco Civil da Internet (Lei nº 12.965/2014) e complementada pelo Código de Processo Penal e pela Lei Geral de Proteção de Dados (Lei nº 13.709/2018).

Aplica-se, sobretudo, a crimes cibernéticos, permitindo o acesso a dados pretéritos ou em tempo real, sempre mediante ordem judicial.

Já a quebra de sigilo telefônico, regulada pela Lei nº 9.296/1996, envolve a interceptação de ligações telefônicas ou acesso a registros de chamadas.

Essa medida exige indispensabilidade à investigação, que o crime tenha pena superior a dois anos, e que não haja outros meios de prova. A interceptação ocorre, em regra, em tempo real, com prazo de 15 dias, prorrogável por igual período.

A jurisprudência do Supremo Tribunal Federal, no Agravo Regimental na Reclamação nº 19464 (Rel. Min. Dias Toffoli, 2020), reafirma que a quebra de sigilo telefônico sem autorização judicial é ilícita, especialmente quando atinge jornalistas e o sigilo da fonte, considerado inviolável pelo artigo 5º, XIV, da Constituição.

Conforme Sakamoto (2023), a distinção essencial entre as duas medidas está no objeto da comunicação: enquanto o sigilo telemático abrange um universo amplo de dados digitais e metadados, o sigilo telefônico restringe-se à rede de telefonia tradicional.

Em síntese, a quebra telemática reflete a adaptação do direito às novas tecnologias, possuindo maior alcance, enquanto a interceptação telefônica segue parâmetros mais rígidos e tradicionais.

Ambas, contudo, devem observar os princípios da proporcionalidade, necessidade e fundamentação judicial, equilibrando a eficiência investigativa com a proteção aos direitos fundamentais.

2.1.2.7 Meios de provas e meios de obtenção de provas

Os meios de prova, conforme Badaró (2017), são instrumentos destinados a trazer ao processo elementos que auxiliem o julgador na busca da verdade real, distinguindo-se dos meios de obtenção de prova, que correspondem aos procedimentos utilizados para coletar tais elementos.

Medidas como busca e apreensão ou interceptação telefônica dependem do sigilo para sua eficácia, embora as provas obtidas devam sempre respeitar o contraditório e a ampla defesa.

Sidi (2016) explica que a quebra de sigilo telemático pode ser compreendida à luz das concepções restritiva e ampliativa de prova atípica.

Antes da Constituição de 1988, as interceptações eram consideradas provas atípicas por falta de previsão legal; com a Constituição e até a edição da Lei nº 9.296/1996, passaram a ser típicas apenas na visão restritiva; e, após a referida lei, tornaram-se típicas em ambas as concepções, em razão da regulamentação expressa do procedimento.

Avelar (2023) reforça que os meios de prova são essenciais à formação do convencimento judicial e à descoberta da verdade dos fatos.

O Código de Processo Penal prevê, de forma exemplificativa, os principais meios de prova como perícias, confissão, depoimentos, reconhecimento, acareação, documentos, indícios e busca e apreensão, todos regidos pelos princípios do contraditório e da ampla defesa.

De acordo com Lopes Jr. (2019), as provas não apenas instruem o processo, mas garantem a efetividade da jurisdição penal, permitindo decisões baseadas na legalidade e na justiça.

Greco (2020) acrescenta que as provas devem ser obtidas de forma técnica e corroboradas por outros elementos, assegurando maior valor probatório, especialmente quando envolvem testemunhos ou documentos colhidos durante a investigação.

2.2 Níveis de Proteção Jurídica da Quebra de Sigilo Telemático

Os mecanismos de quebra de sigilo telemático variam conforme a natureza das informações protegidas, afetando em diferentes graus as garantias constitucionais.

As formas mais invasivas são as interceptações telemáticas e as violações de comunicações armazenadas, seguidas pela apreensão de conteúdos, acesso a metadados e, por último, dados cadastrais.

A Constituição Federal, em seu artigo 5º, incisos X e XII, assegura a proteção à intimidade e ao sigilo das comunicações, cabendo ao Estado intervir apenas nos casos excepcionais previstos em lei.

Nesse sentido, o Supremo Tribunal Federal, no RE 418.416/SC, entendeu que a inviolabilidade protege o fluxo da comunicação, e não o conteúdo em si, sendo legítima a apreensão de suportes físicos contendo dados digitais desde que autorizada judicialmente.

A jurisprudência do Superior Tribunal de Justiça, no HC 315.220/RS (2015), reforçou a aplicação do princípio da proporcionalidade ao anular quebra de sigilo de e-mails de uma década, por ausência de fundamentação e excesso temporal.

Greco (2020) e Prado (2017) criticam ainda a limitação da interceptação apenas a crimes punidos com reclusão, sustentando que o critério é impreciso e pode inviabilizar a investigação de delitos eletrônicos de menor gravidade.

Por fim, Sidi (2016) observa que, sob o ponto de vista técnico, é impossível distinguir comunicações em trânsito das armazenadas, pois o armazenamento é etapa necessária da transmissão digital.

Assim, o Marco Civil da Internet (Lei nº 12.965/2014) cria um paradoxo jurídico, pois confere alta proteção às mensagens em trânsito, mas flexibiliza o acesso às comunicações armazenadas, permitindo uma intromissão potencialmente desproporcional à proteção constitucional do sigilo.

3 CONSIDERAÇÕES FINAIS

Conforme exposto, portanto, qualquer tentativa de harmonizar o tratamento jurídico das comunicações telemáticas em fluxo e armazenadas depende do reconhecimento de que todas estão abrangidas pela proteção do artigo 5º, XII, da Constituição Federal.

Para garantir amparo jurídico, é necessário promover alterações legislativas no Marco Civil da Internet ou em outro diploma legal, criando regras específicas para a quebra de sigilo de comunicações armazenadas.

Essa regulamentação deve prever que a medida tenha finalidade processual penal e baseie-se em indícios razoáveis de autoria ou participação no crime investigado.

As comunicações telemáticas armazenadas continuam protegidas constitucionalmente e só podem ser acessadas mediante decisão judicial fundamentada, sob pena de ilicitude da prova.

O avanço tecnológico transformou a forma de comunicação e armazenamento de informações, impactando o processo penal, que passou a recorrer a meios digitais para obtenção de provas.

Contudo, a legislação processual não acompanhou esse avanço, gerando lacunas supridas por decisões judiciais sem padronização e com risco de abusos.

A quebra de sigilo telemático envolve o acesso a informações sigilosas de diferentes naturezas no contexto investigativo, impactando garantias fundamentais em diferentes intensidades.

As principais modalidades incluem interceptação, acesso a comunicações armazenadas, apreensão de conteúdos diversos, metadados e informações cadastrais.

As comunicações telemáticas têm maior proteção constitucional pelo artigo 5º, XII, da Constituição. Parte da doutrina ainda entende que a proteção se aplica apenas a comunicações em curso, mas essa interpretação é defasada frente à realidade tecnológica, pois reduz a tutela das mensagens armazenadas.

O sigilo constitucional abrange comunicações em curso e armazenadas, mas há dificuldade quanto aos dados em posse de terceiros, como provedores de serviço, o que reforça a necessidade de um marco legal mais claro.

Para garantir segurança jurídica e uniformidade, o ordenamento deve prever normas específicas para o acesso a comunicações armazenadas. O Marco Civil da Internet menciona o tema, mas de forma genérica, sendo necessária uma regulamentação própria, coexistente com a Lei nº 9.296/1996.

Conclui-se que a evolução tecnológica impõe a necessidade de atualização do arcabouço jurídico, de modo a equilibrar a efetividade das investigações criminais com a tutela dos direitos fundamentais, assegurando que a quebra de sigilo telemático seja medida excepcional, devidamente motivada e estritamente proporcional à finalidade investigativa.

REFERÊNCIAS

ALVES, Daniel de Almeida. O direito à privacidade, intimidade e proteção de dados dos trabalhadores perante o avanço tecnológico. 2023.

ANTONIALLI, Dennys; ABREU, Jacqueline de Souza. O conto do baú do tesouro: a expansão da vigilância pela evolução e popularização de celulares no Brasil. InternetLab, 2018.

BADARÓ, Gustavo. Processo penal. 5. ed. São Paulo: Revista dos Tribunais, 2017.

BARROSO, Luís Roberto. Curso de direito constitucional contemporâneo. 9. ed. São Paulo: Saraiva, 2019.

BRASIL. Constituição da República Federativa do Brasil de 1988.

BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal.

BRASIL. Decreto nº 8.771, de 11 de maio de 2016.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet.

BRASIL. Lei nº 9.296, de 24 de julho de 1996.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).

BRASIL. Lei nº 12.850, de 2 de agosto de 2013.

DONEDA, Danilo. Da proteção de dados à proteção da privacidade: uma análise do Marco Civil da Internet. Revista Brasileira de Direito, 2015.

FERRAZ JR., Tércio Sampaio. Direitos fundamentais e processo penal na era digital: doutrina e prática em debate.2018

GONÇALVES, Guilherme Libardi et al. Caracterização de tweets de senadores, governadores e convidados durante a CPI da Pandemia: uma análise através das principais hashtags. 2022.

GRECO, Rogério. Direito penal: parte geral. 20. ed. Rio de Janeiro: Impetus, 2020.

KHEDI, André Pires de Andrade. Sigilo das comunicações e de dados. São Paulo: Revista dos Tribunais, 2008.

PRADO, Luiz Regis. Curso de direito penal brasileiro. Vol. I. 15. ed. São Paulo: Revista dos Tribunais, 2017.

QUITO, Carina. Direito, processo e tecnologia. 2. ed. 2022.

RAPÔSO, Cláudio Filipe Lima et al. LGPD – Lei Geral de Proteção de Dados Pessoais em tecnologia da informação: revisão sistemática. 2019.

ROSSINI, Augusto Eduardo de Souza. Informática, telemática e direito penal. São Paulo: Memória 2004.

SIDI, Ricardo. A interceptação das comunicações telemáticas no processo penal. Belo Horizonte: D'Plácido, 2016..

STF, Reclamação nº 75093 AgR-ED. Relator: Min. André Mendonça. Segunda Turma. Julgado em: 26 maio 2025.

STF, Reclamação nº 19464 SP 8620187-27.2015.1.00.0000. Relator: Min. Dias Toffoli. Segunda Turma, Julgado em: 10 out. 2020.

STF. Reclamação 418.416/SC. Relator: Ministro Sepúlveda Pertence. Tribunal Pleno. Julgamento: 10 mai. 2006.

STJ. Habeas Corpus 315.220/RS. Relatora: Ministra Maria Thereza de Assis Moura. Sexta Turma. Julgamento: 6 fev. 2015.

TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: construção e aplicação. Juiz de Editar, 2016.

VAZ, Denise Provasi. Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório. 2012.

VELLOSO, Fernando. Informática: conceitos básicos. Rio de Janeiro: Elsevier Brasil, 2014.