FACULDADE FASIPE CUIABÁ
CURSO DE DIREITO

YASMIN CAROLINE DA COSTA CARVALHO

A QUEBRA DE SIGILO TELEMÁTICO: ANÁLISE JURISPRUDENCIAL, DOUTRINÁRIA E LEGAL

Cuiabá/MT

2025

CURSO DE DIREITO

YASMIN CAROLINE DA COSTA CARVALHO

A QUEBRA DE SIGILO TELEMÁTICO: ANÁLISE JURISPRUDENCIAL, DOUTRINÁRIA E LEGAL

Trabalho de Conclusão de Curso apresentado à Banca Avaliadora do Departamento de Direito, da Faculdade Fasipe Cuiabá, como requisito para a obtenção do título de Bacharel em Direito.

Orientadora: Prof. Me. Mariana Carolina Deluque Rocha

Cuiabá/MT
2025

YASMIN CAROLINE DA COSTA CARVALHO

A QUEBRA DE SIGILO TELEMÁTICO: ANÁLISE JURISPRUDENCIAL, DOUTRINÁRIA E LEGAL

Trabalho de Conclusão de Curso apresentado à Banca Avaliadora do Curso de Direito – da Faculdade Fasipe Cuiabá como requisito para a obtenção do título de Bacharel em Direito.

Aprovada em 24/06/2025.

Professora Orientadora: Me. Mariana Carolina Deluque Rocha
Coordenadora do Curso de Direito – FASIPE

Professor Avaliador: Esp. Delcio Julio Bento Junior
Departamento de Direito – FASIPE

Professor Avaliador: Me. Thomas Ubirajara Caldas de Arruda
Departamento de Dirreito – FASIPE

Cuiabá/MT
2025

DEDICATÓRIA

À minha mãe, meu maior exemplo de vida, que, entre noites exaustivas de plantões e jornadas de sacrifício, possibilitou, com o fruto de seu esforço incansável, que eu concluísse esta etapa tão importante da minha formação. Sua dedicação e coragem sustentaram cada passo da minha trajetória acadêmica e são, até hoje, a luz que me guia.

AGRADECIMENTOS

- Agradeço, primeiramente, a Deus, por ter me sustentado nos momentos mais desafiadores e me concedido forças para seguir firme nesta caminhada.
- Ao meu padrasto Léo, que nos dias de desânimo soube me levantar, me motivar e me lembrar do quanto sou capaz.
- Ao meu avô Vila, que sempre acreditou no potencial de sua neta e, com os olhos cheios de orgulho, acompanhou cada passo desta jornada.
- À minha prima Larissa e à minha amiga Maria, por estarem presentes em cada etapa deste processo, assistindo meus vídeos, ouvindo minhas angústias e, acreditando em mim.
- Aos professores, em especial minha orientadora, que compartilhou conhecimento, e contribuiu de forma essencial para a minha formação jurídica.
- À instituição de ensino, pelo espaço de crescimento acadêmico, pelas oportunidades e pelo suporte ao longo desses anos.
- A todos que, direta ou indiretamente, fizeram parte desta caminhada, meu sincero e profundo agradecimento.

‘

EPÍGRAFE

‘’Não fui eu que ordenei a você? Seja forte e corajoso! Não se apavore nem desanime, pois o Senhor, o seu Deus, estará com você por onde você andar’’.

Josué 1:9.

CARVALHO, Yasmin Caroline da Costa. **A Quebra de Sigilo Telemático: Análise jurisprudencial, doutrinária e legal.** 2025. 46 F. Trabalho de Conclusão de Curso – Faculdade Fasipe Cuiabá.

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.

CARVALHO, Yasmin Caroline da Costa. **Telematic Secrecy Breakdown: Case Law, Doctrine and Legal Analysis**. 2025. 46 F. Final Course Work – Faculdade Fasipe Cuiabá.

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

SUMÁRIO

1. INTRODUÇÃO 9
2. QUEBRA DE SIGILO TELEMÁTICO 13
2.1 Inviolabilidade do sigilo 14
2.2 Características e espécies jurídicas 17
2.2.1 Interceptações telemáticas 19
2.2.2 Comunicações telemáticas armazenadas 23
2.2.3 Coleta de dados 24
2.2.4 Metadados 26
2.2.5 Dados cadastrais 28
2.2.6 Quebra de sigilo telemático e quebra de sigilo telefônico 30
2.2.7 Meios de provas e meios de obtenção de provas 33
3. NÍVEIS DE PROTEÇÃO JURÍDICA NA QUEBRA DE SIGILO TELEMÁTICO 36
4. CONSIDERAÇÕES FINAIS 41
REFERÊNCIAS 44

1. INTRODUÇÃO

O desenvolvimento tecnológico transformou consideravelmente a maneira como ocorre a interação entre o mundo e a sociedade. Na sociedade da informação, o desenvolvimento ocorre desde o século XX, ao qual a tecnologia se estabelece nos diversos aspectos da vida humana.

A década de 1980 foi marcada com o uso de computadores, através da popularização dos computadores e a expansão da internet para além dos ambientes acadêmico e telefônico, culminando na proliferação de smartphones, notebooks e outros dispositivos.

Esta evolução modificou profundamente as formas de comunicação e o armazenamento de dados pessoais, permitindo a coleta de informações em larga escala, em dispositivos móveis, computadores e servidores, o que ampliou, de forma significativa, as possibilidades de vigilância sobre as atividades humanas.

Neste contexto, o direito penal também passou a utilizar os avanços tecnológicos a seu favor, sendo possível afirmar que os hábitos sociais relacionados à tecnologia alteraram significativamente os métodos de investigação criminal e de obtenção de provas para fins processuais penais, colocando a tecnologia e a internet no centro das discussões sobre o sistema penal contemporâneo.

Contudo, apesar desse avanço tecnológico, o Brasil ainda está avançando de forma restrita na regulamentação das provas digitais e dos métodos de coleta de evidências no processo penal, especialmente no que diz respeito ao uso de tecnologias de comunicação e da internet.

Importante observar que a Constituição Federal, em seu artigo 5º, inciso XII, estabelece a inviolabilidade das comunicações e do sigilo de dados, permitindo sua relativização apenas mediante ordem judicial e nas hipóteses legalmente previstas, especialmente para fins de investigação criminal ou instrução processual penal.

Neste cenário, a Lei nº 9.296, de 24 de julho de 1996, surgiu com o objetivo de regulamentar o artigo constitucional mencionado, estabelecendo normas para a interceptação de comunicações telefônicas e telemáticas, e disciplinando a possibilidade de quebra de sigilo de comunicações.

Posteriormente, a Lei nº 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet, foi sancionada com a finalidade de regular a utilização da internet no Brasil, estabelecendo princípios, garantias, direitos e deveres para os usuários, bem como disciplinando a atuação de provedores.

Dentre suas disposições mais relevantes, destaca-se a proteção das informações pessoais dos usuários e dos registros de acesso, e o compartilhamento dessas informações com as autoridades públicas só pode acontecer mediante ordem judicial. Ademais, o Marco Civil regulamentou a possibilidade de quebra do sigilo das comunicações armazenadas, consolidando-se como marco normativo importante, embora não exauriente.

Apesar de um grande avanço na seara digital, ainda persiste evidente insuficiência normativa para tratar adequadamente das provas digitais e dos procedimentos para sua obtenção. A lacuna é parcialmente preenchida pela aplicação do artigo 240 do Código de Processo Penal, que estabelece as diretrizes para busca e apreensão, tradicionalmente direcionadas à coleta de objetos físicos como meios de provas, mas que, na prática, vêm sendo utilizadas como fundamento jurídico para a apreensão e violação de sigilos de informações contidas em aparelhos móveis, computadores e servidores confiscados.

Todavia, é inegável que esse dispositivo legal se mostra inadequado para lidar com a complexidade das questões que emergem do processo penal na sociedade da informação, marcada pelo uso crescente e sofisticado da tecnologia.

A ausência de legislação específica sobre a coleta e o tratamento de provas digitais, gera instabilidade jurídica e permite um uso exagerado e, em alguns casos, abusivos da supervisão governamental, prejudicando a salvaguarda dos direitos fundamentais à privacidade e ao sigilo das comunicações, garantidos constitucionalmente.

Diante disso, é imprescindível analisar quais são os limites das quebras de sigilo denominadas telemáticas em relação a essas garantias constitucionais, ao qual tem levado a um protagonismo do Poder Judiciário, que, em decisões esparsas e muitas vezes divergentes, busca estabelecer parâmetros para a quebra de sigilo e a apreensão de dados digitais.

No campo constitucional brasileiro, a doutrina de Luís Roberto Barroso enfatiza que o sigilo das comunicações é uma garantia fundamental revestida de força normativa máxima, cuja relativização apenas se justifica mediante decisão judicial fundamentada e na estrita

observância da legislação. Assim, qualquer tentativa de ampliação ou flexibilização desse direito, sem respaldo normativo adequado, representa grave risco à ordem constitucional e ao Estado Democrático de Direito.

O Superior Tribunal de Justiça já consolidou entendimento no sentido de que o acesso a dados armazenados, como registros de conexão e de acesso a aplicações de internet, depende de autorização judicial expressa e fundamentada, sendo nulas as provas obtidas em desrespeito a esse requisito.

Além disso, embora não haja norma específica que regulamente a busca e apreensão de dados digitais, é consenso nos tribunais que a simples aplicação do artigo 240 do Código de Processo Penal não é suficiente para validar essas operações, especialmente considerando a complexidade das informações armazenadas digitalmente.

Ademais, a jurisprudência brasileira tem reforçado a importância de se garantir a inviolabilidade dos dados pessoais, em linha com a evolução legislativa que resultou na promulgação da Lei Geral de Proteção de Dados (LGPD) – Lei nº 13.709/2018, a qual, embora de caráter predominantemente civil e administrativo, reforça a necessidade de tratamento adequado e proporcional das informações pessoais, inclusive na seara penal.

A análise proposta destaca, ainda, a importância de diferenciar a quebra de sigilo telemático da quebra de sigilo telefônico. Embora apresentem características semelhantes, são fenômenos distintos, demandando regulamentações e procedimentos específicos, dada a natureza diversa das informações envolvidas e os potenciais impactos sobre os direitos fundamentais dos indivíduos.

A diferenciação é fundamental, tendo em vista que as comunicações em tempo real, pela sua natureza efêmera e direta, demandam um regime jurídico próprio, distinto daquele aplicável às comunicações e aos dados que permanecem armazenados, muitas vezes por longos períodos, e que podem ser objeto de acesso posterior pelas autoridades estatais.

Assim, uma abordagem que reconheça e respeite essas especificidades é essencial para assegurar a adequada proteção dos direitos fundamentais à privacidade e ao sigilo das comunicações, bem como para garantir a legitimidade e a eficácia das medidas de investigação no âmbito do processo penal.

Por fim, o presente estudo tem como objetivo central a análise das quebras de sigilo envolvendo comunicações telemáticas, com especial atenção à necessidade de se estabelecer distinções claras entre os diferentes níveis de proteção conferidos, tanto às comunicações realizadas em tempo real quanto àquelas que permanecem armazenadas pelos usuários em ambientes digitais.

Este estudo utiliza a metodologia de pesquisa bibliográfica sendo baseada em materiais já elaborados, em especial, código penal, artigos científicos, doutrinas e julgados, pois a principal vantagem da pesquisa bibliográfica consiste que as pesquisas sejam desenvolvidas exclusivamente de referencial bibliográfico.

A pesquisa bibliográfica constitui uma etapa essencial na construção do conhecimento científico, pois permite a análise crítica de obras já publicadas sobre o tema investigado. Este tipo de pesquisa baseia-se no levantamento e na interpretação de contribuições teóricas existentes, possibilitando a formulação de uma base sólida para o desenvolvimento do trabalho. Ao reunir conceitos, posicionamentos doutrinários e entendimentos consolidados, a pesquisa bibliográfica viabiliza a compreensão aprofundada do objeto de estudo, conferindo-lhe respaldo teórico e metodológico.

Além disso, denota-se da pesquisa qualitativa, que possibilita liberdade teórica e metodológica, ao qual os limites de sua iniciativa são fixados pelas condições exigidas a um trabalho científico, contudo tem-se uma estrutura coerente, lógica, plausível e com e nível de objetivação suficiente para de merecer a aprovação dos cientistas em um processo intersubjetivo de apreciação.

Vaz (2019, p.08) destaca que para obter excelência na pesquisa qualitativa, é necessário credibilidade, no sentido de validade interna, ou seja, apresentar resultados dignos de confiança e explicitação cuidadosa da metodologia, detalhando minuciosamente como a pesquisa foi realizada e, por fim, relevância das questões de pesquisa, em relação a estudos anteriores.

O lapso temporal adotado nesta pesquisa contempla aproximadamente os últimos 20 anos, abrangendo, portanto, obras publicadas desde o início desse período até os dias atuais. O objetivo é garantir a atualização e a relevância das informações analisadas, permitindo uma compreensão contextualizada no que diz respeito às quebras de sigilo telemático e à evolução desse instituto ao longo do tempo.

Nesse contexto, a análise bibliográfica e jurisprudencial realizada considera as principais decisões dos tribunais, com ênfase na interpretação dos direitos fundamentais, como a intimidade e o sigilo das comunicações frente às necessidades investigativas do Estado. Dessa forma, busca-se oferecer uma visão crítica e atualizada sobre as quebras de sigilo telemático no processo penal, considerando os avanços tecnológicos, os debates jurídicos e os limites constitucionais envolvidos.

2– QUEBRA DE SIGILO TELEMÁTICO

Consoante aos ensinamentos do doutrinador Doneda (2015, p. 18), a quebra de sigilo telemático consiste em medida judicial que autoriza o acesso a dados armazenados em meios eletrônicos, especialmente aqueles sob a guarda de provedores de aplicações de internet, como redes sociais, correios eletrônicos e serviços de armazenamento em nuvem, além de dados contidos em dispositivos físicos, tais como smartphones, computadores e chips de operadora.

Esta medida configura relevante instrumento de investigação, cuja utilização, entretanto, deve observar os limites constitucionais e legais impostos pela ordem jurídica.

No plano constitucional, a medida encontra amparo no artigo 5º, inciso XII, da Constituição Federal, que assegura a inviolabilidade do sigilo da correspondência, das comunicações telegráficas, de dados e das comunicações telefônicas, permitindo sua restrição apenas mediante ordem judicial e nas hipóteses e formas previstas em lei, para fins de investigação criminal ou instrução processual.

No âmbito infraconstitucional, destaca-se como marco normativo fundamental a Lei nº 12.965/2014, o denominado Marco Civil da Internet, que, em seu artigo 10, § 2º, estabelece que o conteúdo de comunicações privadas somente poderá ser disponibilizado mediante ordem judicial. 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.

Na visão de Doneda (2015, p. 19), a quebra de sigilo telemático não se restringe ao acesso ao conteúdo de mensagens eletrônicas, mas abrange também uma ampla gama de dados armazenados, como listas de contatos, agendas, arquivos digitais, registros de localização, histórico de navegação, de buscas e de compras online.

Segundo o referido autor, tais informações, ainda que não revelem diretamente o conteúdo comunicacional, permitem traçar padrões de comportamento, preferências e hábitos

do indivíduo, razão pela qual demandam proteção legal reforçada, em respeito aos direitos fundamentais à intimidade e à privacidade.

Ainda, como ilustra Sayão (2025, p .17), a carência de informações gera insegurança jurídica e propicia um uso excessivo e, por vezes, abusivo da fiscalização estatal, o que compromete a proteção dos direitos fundamentais à privacidade e ao sigilo das comunicações, constitucionalmente assegurados.

Em se tratando de dados armazenados em dispositivos físicos, como celulares e computadores, a sua apreensão e posterior análise devem obedecer aos procedimentos estabelecidos nos artigos 240 e seguintes do Código de Processo Penal, que disciplinam as medidas de busca e apreensão, a qual será domiciliar ou pessoal. De acordo com o artigo 240, § 1º, do referido código, proceder-se-á à busca domiciliar, quando fundadas razões a autorizarem [...], ou seja, mediante autorização judicial.

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.

Ainda, conforme pontua Doneda (2015, p. 22), a quebra de sigilo telemático, embora constitua instrumento imprescindível para a persecução penal contemporânea, deve ser manejada com extrema cautela, observando os parâmetros constitucionais e legais vigentes, de modo a assegurar a harmonização entre a eficiência da atividade investigativa estatal e a proteção dos direitos fundamentais do indivíduo, pilares basilares do Estado Democrático de Direito.

2.1 - Inviolabilidade do sigilo

Aduz o texto normativo da Constituição Federal de 1988:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> XII - e inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (BRASIL, 1996).

Esse dispositivo assegura a proteção constitucional da privacidade, garantindo que as comunicações permaneçam protegidas contra qualquer violação. Todavia, admite-se a quebra do sigilo das comunicações telefônicas, mediante autorização judicial, observando os limites

legais previstos, visando o equilíbrio entre o direito à intimidade e a necessidade do Estado em realizar investigações criminais e processuais penais.

A evolução da tecnologia e novas formas de comunicação, segundo Alves (2023, p. 19), é produto indispensável na interpretação do texto constitucional indissociável a época em que se vivia um momento histórico em que as comunicações eram essencialmente telefônicas e a internet sequer tinha ainda uso doméstico.

Conforme afirma Sidi (2016, p.15) o Brasil ainda caminha de forma limitada na regulamentação das provas digitais e das formas de coleta de evidências no âmbito do processo penal, sobretudo no que se refere ao emprego de tecnologias de comunicação e ao uso da internet.

Ainda destaca Tomasevicius Filho (2016, p.19), que a proteção dos dados cadastrais dos usuários e dos registros de acesso, cujo fornecimento às autoridades públicas depende, necessariamente, de ordem judicial.

Ferraz Jr. (2018, p. 16) entende que há reconhecido entendimento nos tribunais de que a aplicação isolada do artigo 240 do Código de Processo Penal não basta para legitimar essas operações, especialmente em face da complexidade das informações armazenadas digitalmente.

No ano de 2017, o tema tratando de Direito, Processo e Tecnologia foi revisitado em debate doutrinário, promovido pelo InternetLab com o apoio institucional da Faculdade de Direito da Universidade de São Paulo.

Na ocasião, ao discorrer sobre as noções de fluxo e resultado da comunicação, Ferraz Jr. (2018, p. 13) ainda observa que a dificuldade hoje existente, no mundo digital, está em lidar separadamente com as noções de fluxo e resultado da comunicação, como se fossem totalmente distintas e dissociadas. Isso porque, segundo os autores, a armazenagem no mundo virtual, ao contrário do mundo físico, não é diferente do próprio fluxo.

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.

Quito (2022, p. 172), em suas ditas, complementa essa análise ao afirmar que o importante não seria propriamente o tempo da transmissão da comunicação, mas a espontaneidade em comunicar-se. Essa fluência, segundo o autor, é fundamental para garantir um ambiente democrático, onde as ideias possam ser trocadas livremente, contribuindo para o fortalecimento da cidadania e da pluralidade de vozes na sociedade.

De acordo com Sidi (2016, p.70), a distinção entre fluxo e resultado, o qual não é mencionada no texto constitucional, não se aplica ao contexto atual, em que as comunicações eletrônicas passam por diversas etapas de armazenamento entre o envio pelo remetente e o recebimento pelo destinatário.

Para o autor, o objeto de proteção do artigo 5º, XII, da Constituição Federal é o conteúdo das comunicações, sem distinção entre as mensagens contemporâneas armazenadas, uma vez que a preservação do conteúdo e dos detalhes não pode ser dissociada do sigilo.

Além disso, a arguição de Sidi (2016, p.72) aponta que a questão tecnológica inviabiliza a delimitação precisa do momento em que a comunicação telemática está efetivamente em fluxo. O exame do objeto de proteção do artigo 5º, XII, da Constituição Federal deve incluir a finalidade do sigilo, que é manter informações em segredo. O que se busca proteger do conhecimento de terceiros é, portanto, o conteúdo da comunicação, pois, sem essa proteção, o sigilo não teria justificativa.

O foco da proteção constitucional visa resguardar, além da intimidade, a liberdade de pensar e expressar ideias sem que pessoas não autorizadas tenham acesso ao que foi dito. Com isso, para a quebra do sigilo é necessário reconhecer que o conteúdo das comunicações estará transmitido ou armazenado.

Assim, a proteção do sigilo prevista no artigo 5º, XII, da Constituição Federal requer uma evolução nas interpretações doutrinárias e na jurisprudência, reconhecendo que o conteúdo das comunicações deve ser mantido em segredo para assegurar a espontaneidade nas interações, pois diante da falta de clareza do artigo mencionado, no que concerne aos limites da exceção ao sigilo das comunicações, a constitucionalidade do parágrafo único do artigo 1º da Lei nº 9.296/1996 foi amplamente debatida nos anos subsequentes à sua promulgação, qual seja:

> Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça (BRASIL, 1996).

Entretanto, o parágrafo único do artigo 1º da Lei nº 9.296/1996 estabelece que o disposto nesta Lei se aplica à interceptação do fluxo de comunicações em sistemas de informática e telemática. Com isso, ao estender as regras das interceptações telefônicas para o fluxo de comunicações em sistemas de informática e telemática, gerou questionamentos quanto à sua compatibilidade com o texto constitucional.

A controvérsia jurídica reside na interpretação do termo "último caso", previsto no artigo 5º, XII, da Constituição Federal, uma vez que a norma menciona expressamente apenas a

interceptação de comunicações telefônicas, sem aludir diretamente às comunicações telemáticas.

Assim, a ampliação dessa previsão por meio de legislação infraconstitucional levantou discussões quanto a um possível excesso normativo e a necessidade de interpretação conforme a Constituição.

2.2 – Características e espécies jurídicas

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

Como destaca Velloso (2014, p. 56), a década de 1980 foi marcada pelo avanço no uso de computadores, impulsionado pela popularização desses dispositivos e pela expansão da internet além dos ambientes acadêmicos e telefônicos.

Esse processo evolutivo culminou na disseminação de equipamentos como smartphones, notebooks e outros dispositivos móveis, que passaram a desempenhar um papel central na comunicação moderna e no armazenamento de informações pessoais e sensíveis.

Conforme esclarece o doutrinador Sidi (2016, p. 69), a comunicação é considerada telemática, em seu sentido jurídico, quando ocorre de forma digital, ou seja, por meio da conversão em séries binárias. Isso independe da estrutura utilizada, desde que não se enquadre nas modalidades específicas de comunicação telefônica e telegráfica.

Refere-se, portanto, às comunicações de dados realizadas por meio da transmissão de sinais binários, em geral pela rede mundial de computadores. Conforme explica Rossini (2004, p. 160):

> (...) observa que a telemática foi o que permitiu a comunicação de uma máquina com a outra, dando origem à chamada Era da Informação, que possui cinco pilares: números, que são usados para representar todas as informações; os números expressos em 0s e 1s; os computadores transformam a informação ao tratar aritmeticamente esses números; os sistemas de comunicação movem os números e, assim, transportam a informação; e computadores e sistemas de comunicação se combinam para formar redes por onde trafegam os dados, sendo a mais conhecida a internet.

Ademais, em relação a Era da Informação, refere-se Vaz (2012, p. 19), da seguinte forma:

> os documentos anteriormente redigidos e arquivados em papel tornaram-se eletrônicos; as músicas foram transferidas do disco de vinil e fia cassete para o formato digital; as fotografias deixaram de ser registradas em filme para também assumirem o

> formato digital; do mesmo modo, a captação de imagens em vídeos; e ainda a comunicação por cartas, bilhetes, telegrama, telefone, foi transmudada em mensagens eletrônicas de texto, e-mails, sistemas VolP, dentre outros.

A quebra de sigilo telemático, em regra, é uma providência de natureza cautelar, uma vez que a eficácia do meio depende do sigilo da medida até sua execução. Badaró (2017, p. 394) destaca que, por essa razão, o requerimento, a admissibilidade e a efetiva realização do meio devem ocorrer sem o conhecimento da parte investigada, sendo o resultado de tal operação posteriormente submetido ao contraditório diferido.

Sob essa órbita, diversas medidas são autorizadas judicialmente e executadas, as quais podem afastar sigilos protegidos tanto pela garantia constitucional à intimidade e à vida privada, prevista no artigo 5º, inciso X, da Constituição Federal assegurando que 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.

Quanto ao sigilo das comunicações, garantido no mesmo artigo, em seu inciso XII, estabelece que é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Assim, desde que haja uma determinação judicial, são autorizadas quebras de sigilo que abrangem tanto as comunicações em tráfego quanto conteúdos já armazenados em dispositivos móveis, computadores e servidores, além de metadados e dados cadastrais.

A confusão terminológica surge da falta de definições legais precisas para cada tipo de quebra e da ausência de rigor no uso de conceitos técnicos.

Apesar do uso indiscriminado do termo para designar diferentes objetos, qualquer quebra de sigilo telemático terá a natureza jurídica de meio de obtenção de prova, funcionando como um instrumento para a investigação e coleta de fontes de prova.

Como ensina Badaró (2017, p. 393), os meios de obtenção de provas, também conhecidos como meios de investigação ou pesquisa de provas, são ferramentas para a coleta de fontes ou elementos de prova.

O único meio de obtenção de prova disciplinado pelo Código de Processo Penal em seus artigos 240 a 250 é a busca e apreensão, existindo outros meios previstos em leis processuais penais especiais, como as interceptações telemáticas, a interceptação ambiental, as quebras de sigilo bancário e fiscal, e a infiltração de agentes em organizações criminosas.

Dessa forma, a promulgação da Lei nº 13.964/2019, popularmente conhecida como Pacote Anticrime, trouxe importantes inovações no campo da persecução penal, entre elas a

criminalização da realização de interceptações ou captações ambientais sem prévia autorização judicial.

Com essa finalidade, foi inserido o artigo 10-A na Lei nº 9.296/1996, que trata das interceptações telefônicas. O novo dispositivo passou a prever sanção penal para a captação ambiental de sinais acústicos, ópticos ou eletromagnéticos voltada à investigação ou instrução de processos criminais realizada sem autorização do Poder Judiciário.

2.2.1 Interceptações telemáticas

Por interceptação, entende-se a intrusão, por terceiros não autorizados, no fluxo de comunicações privadas entre duas ou mais pessoas enquanto estas ocorrem. Consoante ao ensinamento de Greco (2020, p. 92), a interceptação consiste na captação da conversa por um terceiro, sem o conhecimento dos interlocutores, interceptação em sentido estrito, ou com o conhecimento de um deles.

Ao realizar a interceptação, esses terceiros não apenas se inserem de forma errônea no fluxo da comunicação, mas também monitoram as interações para obter acesso ao conteúdo transmitido durante um determinado período.

Essa prática trás questões significativas sobre a proteção da privacidade e a legalidade das intervenções nas comunicações pessoais. Conforme ensina Vaz (2012, p. 100):

> A medida consiste na captação de dados que estejam em trânsito por uma rede de dispositivos eletrônicos, podendo recair sobre um determinado serviço, como o correio eletrônico, ou sobre a troca de dados a partir de um determinado endereço de IP, caso em que são coletadas todas as mensagens de correio eletrônico, bem como as conversas mantidas por meio de comunicadores instantâneos, VoIP etc.

As interceptações telemáticas encontram respaldo no artigo 1º, parágrafo único, da Lei nº 9.296/1996, o qual compreende que as interpretações contidas naquele diploma legal quanto às interceptações telefônicas estendem-se às interceptações de comunicações telemáticas. Destaca-se:

> Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça. Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática (BRASIL, 1996).

Sobre as interceptações telemáticas, Sidi (2016, p. 61) afirma que se trata de uma providência cautelar que constitui um meio de obtenção de prova, sendo o material coletado,

via de regra, armazenado em mídias como CD, DVD ou pendrive, configurando-se como um meio de prova documental que será inserido no processo.

Khedi (2008, p.242) trata sobre a temática, abordando, principalmente, duas correntes doutrinárias. A primeira defende que o texto constitucional abrange quatro modalidades de comunicação: comunicação postal, comunicação telegráfica, comunicação de dados e comunicação telefônica.

Segundo essa perspectiva, a exceção constitucional ‘’salvo, no último caso’’ se aplica apenas às comunicações telefônicas, o que tornaria as demais formas, incluindo as comunicações de dados, absolutamente invioláveis.

Para a segunda corrente, o texto constitucional teria separado as formas de comunicação em dois blocos: comunicação postal e telegráfica, de um lado, e comunicação de dados e telefônica, de outro. Assim, a exceção constitucional ao sigilo das comunicações seria aplicável apenas ao segundo bloco, ou seja, às comunicações de dados e telefônicas.

Conforme Badaró (2017, p. 492), a interceptação de comunicações telefônicas e telemáticas constitui um meio legítimo de obtenção de provas no processo penal, desde que respeitados os limites impostos pela Constituição e pela legislação infraconstitucional. Diante do inevitável avanço tecnológico, essa corrente prevaleceu.

Nesse interim, o autor destaca que uma interpretação realista da norma constitucional não poderia afastar a possibilidade de interceptação das comunicações telemáticas, uma vez que não se pode considerar uma norma constitucional isolada de seu contexto histórico, social e político, mormente em temas que envolvem a evolução tecnológica.

De acordo com Quito (2022, p. 167), as interceptações de comunicações telemáticas tiveram o seu uso alargado, sendo hoje tão ou mais frequentes do que as próprias interceptações telefônicas.

Esse entendimento doutrinário foi refletido na jurisprudência, que se consolidou para admitir essa modalidade de interceptação sob o mesmo regime dos monitoramentos telefônicos. Veja-se:

> DIREITO PROCESSUAL PENAL. AGRAVO REGIMENTAL. RECURSO ORDINÁRIO EM HABEAS CORPUS. INTERCEPTAÇÃO TELEFÔNICA E TELEMÁTICA. FUNDAMENTAÇÃO DAS DECISÕES. AGRAVO DESPROVIDO.1. Agravo regimental interposto contra decisão que rejeitou embargos de declaração em recurso ordinário em habeas corpus no qual se pleiteava a nulidade das decisões de quebra de sigilo telefônico e telemático por alegada falta de fundamentação. 2. As decisões impugnadas autorizaram a interceptação telefônica e a

> quebra de sigilo de dados com base em indícios de crimes graves, como exploração de jogos de azar, peculato e corrupção, envolvendo policiais militares e particulares. Tese de julgamento: "1. As decisões de interceptação telefônica e suas prorrogações não exigem fundamentação exaustiva, bastando a demonstração dos requisitos legais. 2. A fundamentação per relationem é válida para prorrogações de interceptação telefônica, desde que os pressupostos da medida sejam mantidos. (STJ - AgRg nos EDcl no RHC n. 157.798/PR, relator Ministro Messod Azulay Neto, Quinta Turma, julgado em 12/2/2025, DJEN de 17/2/2025.) (grifo nosso.)

Os requisitos e procedimentos para a implementação dessa medida investigativa estão estabelecidos na Lei n.º 9.296/1996, o que caracteriza a interceptação telemática como um método típico de obtenção de provas, sujeito às garantias constitucionais e legais pertinentes.

O artigo 2º da referida lei, define requisitos que traduzem em termos legais critérios de proporcionalidade, os quais foram detalhados por Barroso (2019, p. 512):

> (..) proporcionalidade também refere-se a um princípio instrumental para aferir a legitimidade das restrições a direitos fundamentais em três etapas, nas quais vai verificar: (i) a adequação de uma medida para produzir determinado resultado, sendo vedado o uso de meio inadequado e invasivo; (ii) a necessidade da providência, ou seja, se houver meios menos gravosos; e (iii) a proporcionalidade em sentido estrito, pela qual se afere se o fim justifica o meio, vale dizer, se o que se ganha mais do que aquilo que se perde ou se sacrifica.

Portanto, nas lições de Barroso, as interceptações somente podem ser autorizadas quando preenchidos três requisitos indispensáveis. Primeiramente, é necessário que existam indícios razoáveis de autoria ou participação em infração penal.

Além disso, conforme o mesmo autor, deve-se demonstrar a imprescindibilidade da medida para a obtenção da prova da infração penal, evidenciando que outros meios seriam inadequados ou insuficientes. E, por fim, o fato investigado deve constituir infração penal punida com reclusão, não se admitindo a interceptação para crimes de menor gravidade.

Já o artigo 3º da Lei n.º 9.296/1996 estabelece quem pode solicitar a medida, permitindo que autoridades policiais e representantes do Ministério Público façam o pedido, além de mencionar que juízes podem determinar sua execução de ofício.

O artigo 4º aborda o conteúdo do requerimento, que pode ser feito por escrito ou oralmente em situações de urgência, e deve demonstrar a necessidade do uso do meio de prova e indicar os métodos a serem utilizados, conforme os requisitos do artigo 2º, abaixo explicitado:

> Art. 4° O pedido de interceptação de comunicação telefônica conterá a demonstração de que a sua realização é necessária à apuração de infração penal, com indicação dos meios a serem empregados.

> § 1° Excepcionalmente, o juiz poderá admitir que o pedido seja formulado verbalmente, desde que estejam presentes os pressupostos que autorizem a interceptação, caso em que a concessão será condicionada à sua redução a termo.
> § 2° O juiz, no prazo máximo de vinte e quatro horas, decidirá sobre o pedido. (BRASIL, 1996).

Ademais, no artigo 5º da mesma lei, determina-se que a decisão que autoriza a medida deve ser fundamentada, sob pena de nulidade, e deve especificar a forma de execução da diligência, não poderá ultrapassar quinze dias, podendo ser renovada por igual período, desde que a indispensabilidade do meio de prova seja comprovada.

Os artigos 8º e 9º estabelecem que as interceptações devem ser registradas em autos separados dos processos de investigação ou ação penal, garantindo o sigilo das diligências e do material obtido, e que qualquer material irrelevante para a persecução criminal deve ser descartado, com a ciência do juiz, a pedido do Ministério Público ou da parte interessada.

Além disso, a lei nº 13.964/1996 inseriu na lei nº 9.296/1996 o artigo 8-A, que tipifica o meio de obtenção de prova diversa, qual seja, a captação ambiental de sinais eletromagnéticos, ópticos ou acústicos. Conforme o dispositivo legal:

> Art. 8º-A. Para investigação ou instrução criminal, poderá ser autorizada pelo juiz, a requerimento da autoridade policial ou do Ministério Público, a captação ambiental de sinais eletromagnéticos, ópticos ou acústicos, quando:
> I - a prova não puder ser feita por outros meios disponíveis e igualmente eficazes; e
> II - houver elementos probatórios razoáveis de autoria e participação em infrações criminais cujas penas máximas sejam superiores a 4 (quatro) anos ou em infrações penais conexas (BRASIL, 1996).

O artigo 10, cuja redação foi recentemente alterada pela Lei n.º 13.964/2019, tipifica como crime, punido com pena de dois a quatro anos de reclusão e multa, a realização de interceptações ou escutas ambientais, ou a quebra de sigilo, sem autorização judicial ou para fins não previstos em lei.

O parágrafo único desse artigo tipifica a conduta de autoridades que ordenam a execução de interceptações ou escutas para fins não autorizados, sujeitando o agente às mesmas penas do caput.

Embora o procedimento probatório esteja relativamente definido na Lei n.º 9.296/1996 em relação às interceptações telefônicas, a legislação não especificou um formato para a execução das interceptações telemáticas, que incluem acessos a registros de conexões, dados de e-mails ou outras plataformas de troca de mensagens online.

Isso demanda uma atuação judicial inovadora e a superação de novos desafios técnicos e linguísticos, permitindo o acesso em tempo real aos fluxos de mensagens dos investigados,

de modo que seus conteúdos possam ser acessados pelas autoridades responsáveis pelas investigações.

É importante ressaltar que a criação de contas espelho, medida utilizada para replicar contas de e-mail ou mensagens, não está prevista na Lei n.º 9.296/1996, nem na Resolução n.º 59/2008 do Conselho Nacional de Justiça, que regulamenta e padroniza rotinas para aprimorar o procedimento de interceptação de comunicações telefônicas e serviços de informática e telemática nos órgãos do Poder Judiciário.

Essa abordagem convencional para solicitar a execução da medida não exclui a possibilidade de acessar o fluxo das comunicações por outros meios técnicos igualmente eficazes.

2.2.2 Comunicações telemáticas armazenadas

Segundo o que fora explicitado por Rapôso (2019, p. 58), a Lei Geral de Proteção de Dados Pessoais, instituída pela Lei nº 13.709/2018, foi criada com o objetivo de resguardar os direitos fundamentais à liberdade, à privacidade e ao livre desenvolvimento da personalidade.

A referida norma regula o tratamento de dados pessoais, sejam eles armazenados em formato físico ou digital, realizado por pessoas naturais ou jurídicas, de direito público ou privado, abrangendo uma ampla gama de operações em meios eletrônicos e não eletrônicos.

Nesse contexto, destaca-se que a Lei nº 9.296/1996, que disciplina a interceptação de comunicações, não prevê expressamente o acesso a comunicações telemáticas armazenadas.

Ainda assim, a liberação do sigilo de mensagens pretéritas, frequentemente armazenadas em servidores, tem sido recorrentemente autorizada no âmbito de investigações criminais, tornando-se uma prática consolidada, embora não isenta de controvérsias jurídicas e constitucionais.

Conforme apontam Abreu e Antonialli (2017, p. 69), a legislação infraconstitucional aborda a questão em dois diplomas legais distintos. Quando o acesso depende de intermediários, como provedores de aplicações de internet que armazenam os dados, aplica-se o artigo 7º, inciso III, do Marco Civil da Internet, que exige ordem judicial, mas não estabelece critérios específicos de prova.

Já quando o acesso ocorre diretamente em dispositivos móveis, computadores ou servidores apreendidos, a base legal é o artigo 240 do Código de Processo Penal, que regula busca e apreensão.

Ao condicionar o acesso a mensagens armazenadas em servidores de provedores apenas à existência de uma ordem judicial, sem impor limites temporais ou outros requisitos, a Lei nº

12.965/2014, Marco Civil da Internet, gera uma contradição, que será discutida em relação as comunicações armazenadas, que por muitas vezes e longos períodos, recebem, na prática investigativa, proteção inferior às comunicações telemáticas em tempo real.

Estas, por sua vez, possuem maior proteção judicial, pois sua interceptação depende do cumprimento de exigências previstas na Lei nº 9.296/1996, geralmente limitadas a um prazo de 15 dias.

Embora a Lei nº 12.965/2014 não tenha definido requisitos específicos para essas quebras de sigilo, o acesso ao conteúdo de comunicações armazenadas, por envolver restrição a direitos fundamentais, deveria observar critérios de proporcionalidade, incluindo seus subprincípios, o que nem sempre ocorre na prática investigativa.

2.2.3 Coleta de dados

A denominada quebra de sigilo telemático frequentemente abrange a liberação de acesso a diversos dados armazenados em dispositivos móveis, computadores ou servidores, incluindo correspondências eletrônicas.

Essas informações abrangem elementos como listas de contatos, calendários de compromissos, fotografias, documentos de texto, arquivos de vídeo e áudio, planilhas eletrônicas, registros de localização, trajetos realizados pelos usuários, histórico de navegação na internet, consultas realizadas em mecanismos de busca, aplicativos instalados, dados relacionados a transações comerciais online, entre outros.

Em resumo, incluem-se todas as formas de dados que podem estar armazenados nos próprios dispositivos dos investigados ou nos servidores de empresas provedoras de aplicações de internet.

Em relação a normativa jurídica acerca do levantamento do sigilo de dados de localização há escassez, inclusive no Marco Civil da Internet, excetuando-se as hipóteses previstas no artigo 13-B do Código de Processo Penal. Esse dispositivo, introduzido ao estatuto processual pela Lei nº 13.344/2016, regula o acesso a tais dados, autorizando que:

> Art. 13-B. Se necessário à prevenção e à repressão dos crimes relacionados ao tráfico de pessoas, o membro do Ministério Público ou o delegado de polícia poderão requisitar, mediante autorização judicial, às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso (BRASIL, 2016).

Todavia, o referido dispositivo torna-se inconstitucional, pois permite restrição à garantia descrita no artigo 5º, inciso X, da Constituição Federal, observa-se:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...) 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 (BRASIL, 1998).

Assim, o acesso a essas informações é frequentemente amparado pelos artigos 240 e seguintes do Código de Processo Penal, que tratam das medidas de busca e apreensão.

Esses dispositivos legais, conforme Vaz (2012, p. 22v), estabelece os requisitos e procedimentos para a realização de tais medidas, garantindo que sejam conduzidas com autorização judicial, exceto em situações de flagrante delito ou consentimento expresso, respeitando os princípios constitucionais de proteção à privacidade e à dignidade da pessoa humana.

Como o Código de Processo Penal foi elaborado para regular a apreensão de objetos materiais, ele é utilizado como base legal para acessar dados armazenados em dispositivos como smartphones, computadores e servidores, desde que a apreensão física seja autorizada por decisão judicial fundamentada, acompanhada de mandado específico.

O mandado de busca deve contar a indicação precisa do local da busca e a delimitação também precisa de seu objeto conforme afirma Drakoulakis (2022, p. 33), não se admitindo interpretações diversas, tampouco ampliação do objeto do mandado durante sua execução.

Ainda de acordo com especificação de Quito (2022, p.172), no caso de dados acessados remotamente em servidores de empresas provedoras de aplicações de internet, as autoridades investigativas e o Judiciário costumam se valer do artigo 240 do Código de Processo Penal. Ademais, argumentou-se que as informações nesses bancos de dados equivalem a documentos, passíveis de apreensão remota ou imprópria.

A falta de regulamentação específica faz com que a quebra do sigilo desses dados, protegidos pela garantia do artigo 5º, X, da Constituição Federal, dependa apenas de uma ordem judicial, independentemente da finalidade da coleta ou de limitações temporais.

Além disso, Alves (2023, p. 21) destaca que com o avanço tecnológico, os smartphones transcendem a função de simples dispositivos para chamadas e mensagens. Eles se tornaram verdadeiros computadores pessoais portáteis, funcionando como extensões da vida de seus usuários, possibilitando o armazenamento de informações que refletem com precisão a identidade e os hábitos de seus proprietários.

Esses dados, no entanto, não se limitam ao conteúdo de comunicações pessoais. É notório que a quebra de sigilo dessas informações pode resultar em significativa invasão da

privacidade, uma vez que possuem a capacidade de revelar um amplo espectro de comportamentos e preferências do indivíduo.

2.2.4 Metadados

O uso de aplicações na internet gera registros que incluem data, hora, localização e endereço de protocolo (IP), conhecidos como metadados. Esses são regulamentados no artigo 5º, VI e VIII, da Lei nº 12.965/2014 do Marco Civil da Internet.

Abreu e Antonialli (2017, p. 23) relatam que o conceito de metadados pode variar. Segundo os autores, todos os dados e registros gerados a partir de uma comunicação que não constituem o seu conteúdo em si, como, por exemplo, data, hora e duração da comunicação, remetente, destinatários, eventuais dados de localização geográfica do dispositivo como a Estação de Rádio Base e códigos de identificação de dispositivos como a Identificação Internacional de Equipamento Móvel – IMEI, são considerados metadados.

Nesse sentido, segundo a Agência Nacional de Telecomunicações (2020), o IMEI é um número de identificação único e global atribuído a cada aparelho celular.

Entretanto, no entendimento de Sidi (2016, p. 294), os metadados referem-se a tais dados como de tráfego, que englobam a identificação do remetente e do destinatário das mensagens, horário de envio, a localização dos interlocutores através de Estações de Rádio Base, a quantidade de bytes transmitidos, volume de áudio (em caso de transmissão de áudio), duração dos diálogos, IPs gerados e o custo da comunicação.

Em síntese, os registros de conexão referem-se ao conjunto de dados que indicam a data, a hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado para enviar e receber informações.

O artigo 10 da Lei nº 12.965/2014 (Marco Civil da Internet), determina que tanto o armazenamento quanto o acesso aos registros ali especificados devem respeitar a proteção à intimidade, à vida privada, à honra e à imagem dos indivíduos, em conformidade com o disposto no artigo 5º, inciso X, da Constituição Federal.

A norma estabelecida no artigo 13 desta mesma lei impõe aos provedores de conexão e de aplicações a obrigação de manter esses registros por, respectivamente, um ano, quando solicitado por autoridades, com ciência do Ministério Público, caso seja necessário para obter ordem judicial que autorize a quebra de sigilo correspondente.

Conforme entendimento de Sayão (2010, p.15), considerando que esses dados estão intrinsecamente ligados às comunicações e às atividades realizadas pelos usuários na internet, os metadados são tratados como informações protegidas.

Assim, sua liberação está condicionada à cláusula de reserva de jurisdição, conforme estipulado expressamente nos artigos 10, § 3º, e 15, § 3º, da Lei nº 12.965/2014 (Marco Civil da Internet), veja -se:

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. [...] § 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição. (grifo nosso)
> Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento. [...] § 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo (BRASIL, 2014) (grifo nosso).

O artigo 22, parágrafo único, da mesma lei, estabelece os requisitos para que uma parte interessada solicite ao Judiciário o acesso aos registros de conexão e de acesso a aplicações de internet, seja âmbito cível ou criminal. Observa-se:

> Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.
> Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:
> I - fundados indícios da ocorrência do ilícito;
> II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e
> III - período ao qual se referem os registros (BRASIL, 2014).

Com isso, os pontos pautados nos três incisos incluem a demonstração de fundamentos plausíveis para a ocorrência de um ilícito, a apresentação de indícios suficientes de autoria ou participação e a comprovação da adequação e proporcionalidade da medida solicitada.

Embora menos rigorosos que os critérios previstos na Lei nº 9.296/1996 da interceptação telefônica, os requisitos do artigo 22 da Lei nº 12.965/2014, Marco Civil da Internet, refletem princípios de proporcionalidade, exigindo que a medida seja necessária, adequada e equilibrada em relação ao objetivo pretendido, de modo a limitar a interferência nas garantias constitucionais de intimidade e vida privada.

No âmbito das investigações parlamentares, a possibilidade de quebra de sigilos, inclusive bancário, fiscal e de dados telemáticos, inclui também o acesso a metadados, cuja análise é essencial para a reconstrução de fluxos de comunicação, identificação de vínculos e mapeamento de ações relevantes à apuração dos fatos.

Nesse sentido, a discussão sobre o acesso às provas digitais no processo penal tem gerado importantes reflexões no Supremo Tribunal Federal.

Em recente julgamento de maio de 2025, o Ministro André Mendonça, relator da Reclamação 75093 AgR-ED, destacou que o pedido dos embargantes se referia ao acesso à integralidade das provas digitais já produzidas, incluindo os metadados extraídos de aparelhos apreendidos:

> EMENTA EMBARGOS DE DECLARAÇÃO EM AGRAVO REGIMENTAL NA RECLAMAÇÃO CONSTITUCIONAL. ACESSO À PROVA DIGITAL. ALEGAÇÃO DE OBSCURIDADE. INEXISTÊNCIA DE VÍCIOS NO ACÓRDÃO. EMBARGOS REJEITADOS. I. CASO EM EXAME. Embargos de declaração opostos contra acórdão da Segunda Turma do Supremo Tribunal Federal que, por unanimidade, negou provimento a agravo regimental interposto em reclamação constitucional. Os embargantes alegam obscuridade, sustentando que o pedido formulado visava exclusivamente ao acesso à integralidade das provas digitais já produzidas nos autos, incluindo os metadados extraídos de aparelhos apreendidos (STF – Rcl 75093 AgR-ED, Relator: Min. ANDRÉ MENDONÇA, Segunda Turma, julgado em 26/05/2025, PROCESSO ELETRÔNICO, DJe-s/n, divulgado em 29/05/2025, publicado em 30/05/2025).

Portanto, conforme explicitado por Gonçalves (2022, p.10), a quebra de sigilo, quando abrange metadados, revela-se uma medida legítima e indispensável para o adequado exercício da função investigatória, permitindo que se obtenham elementos informativos essenciais à elucidação dos fatos, sem, contudo, violar indevidamente o conteúdo das comunicações protegidas constitucionalmente.

2.2.5 Dados cadastrais

Assim como os registros de conexão e de acesso a aplicações, o artigo 10 da Lei nº 12.965/2014 (Marco Civil da Internet) estabelece que o acesso aos dados cadastrais dos usuários da internet deve, como regra, observar a garantia prevista no artigo 5º, inciso X, da Constituição Federal.

O Decreto nº 8.771/2016, define, em seu artigo 11, § 2º, incisos I a III, o que constitui dados cadastrais: informações sobre filiação, endereço e qualificação pessoal do usuário, esta última compreendendo nome, prenome, estado civil e profissão. Por sua vez, o § 1º do mesmo

artigo isenta os provedores que não coletam tais dados da obrigação de fornecê-los às autoridades, desde que comuniquem formalmente essa situação à parte requisitante.

O artigo 10, caput, da Lei nº 12.965/2014 (Marco Civil da Internet) estabelece que o fornecimento de dados pessoais deve respeitar a proteção à intimidade, à vida privada, à honra e à imagem dos indivíduos. Essa é a regra geral, com exceção prevista no § 3º do mesmo artigo, que permite o acesso a dados cadastrais por autoridades administrativas com competência legal para a solicitação.

No contexto da proteção de dados e da regulamentação do acesso a informações cadastrais, o Decreto nº 8.771, de 11 de maio de 2016, estabelece diretrizes claras para as autoridades administrativas.

Conforme disposto no artigo 11 do mencionado decreto, as autoridades administrativas a que se refere o artigo 10, § 3º da Lei nº 12.965, de 2014, indicarão o fundamento legal de competência expressa para o acesso e a motivação para o pedido de acesso aos dados cadastrais.

Esse dispositivo reforça a necessidade de transparência e embasamento legal no tratamento de dados pessoais, alinhando-se aos princípios do Marco Civil da Internet. A exigência de motivação expressa visa garantir que o acesso a informações sensíveis ocorra de forma justificada, respeitando os direitos fundamentais à privacidade e à proteção de dados, conforme preconiza a legislação brasileira, lei nº 12.965/2014.

Quito (2022, p.175) entende que a reserva de jurisdição deve ser o princípio norteador para a liberação desses dados, sendo o acesso direto uma exceção, permitido somente em casos expressamente previstos em lei, quando a gravidade das infrações investigadas justifique a priorização da eficiência na persecução penal em detrimento da garantia constitucional.

As hipóteses excepcionais estão previstas em dispositivos legais específicos, como o artigo 17-B da Lei nº 6.613/1998 (alterada pela Lei nº 12.683/2012), que trata dos crimes de lavagem de dinheiro.

Além disso, tem-se o artigo 15 da Lei nº 12.850/2013, que regula a atuação de organizações criminosas e o artigo 13-A do Código de Processo Penal, que disciplina o acesso a dados cadastrais nas investigações de crimes previstos nos artigos 148 (Sequestro e Cárcere Privado) , 149 (Redução a Condição Análoga à de Escravo), 149-A (Tráfico de Pessoas), 158 (Extorsão), 185 § 3º (Extorsão mediante restrição da liberdade da vítima), e 159 (Extorsão mediante Sequestro) do Código Penal, além do artigo 239 do Estatuto da Criança e do Adolescente.

Os artigos 13-A e 13-B, conforme já mencionado, foram inseridos no Código de Processo Penal pela Lei nº 13.344/2016, com o objetivo de tornar as investigações criminais

mais eficazes na apuração de delitos como sequestro e cárcere privado, redução à condição análoga à de escravo, tráfico de pessoas e extorsão mediante sequestro, crimes de elevada gravidade, que possuem como elemento comum a restrição contínua da liberdade de locomoção das vítimas.

Por se tratarem de exceções, consideramos que, em conformidade com a garantia do artigo 5º, inciso X, da Constituição Federal, essas normas devem ser interpretadas de forma restritiva, limitando o acesso direto a dados cadastrais exclusivamente às investigações dos crimes expressamente mencionados nesses dispositivos legais.

Abreu e Antonialli (2018, p. 33), destacam que as normas que previram a desnecessidade de ordem judicial para o acesso a dados cadastrais são fruto de recentes reformas legislativas que atendem a pressões das autoridades administrativas para ter acesso direto aos dados, visando ao aumento da eficiência das investigações, sobretudo em termos de rapidez.

Ressalta os doutrinadores que, nesse mesmo das modificações legislativas, essas autoridades administrativas já defendiam o acesso direto a dados cadastrais, ao argumento de que tais informações não receberiam a proteção constitucional do artigo 5º, X ou XII.

2.2.6 Quebra de sigilo telemático e quebra de sigilo telefônico

A quebra de sigilo telemático e a quebra de sigilo telefônico são medidas investigativas de caráter excepcional no ordenamento jurídico brasileiro, destinadas a acessar comunicações privadas para a produção de provas em processos criminais.

Ambas encontram amparo no artigo 5º, inciso XII, da Constituição Federal, que assegura o sigilo das comunicações, salvo por ordem judicial fundamentada, em casos previstos em lei e para fins de investigação criminal ou instrução processual penal.

Contudo, tais medidas distinguem-se quanto ao objeto, finalidade, regulamentação legal e procedimentos, refletindo as especificidades das tecnologias de comunicação envolvidas e os limites impostos pelo ordenamento jurídico para a proteção dos direitos fundamentais.

Como se refere Fares (2019, p.34), a quebra de sigilo telemático se dá ao acesso, mediante autorização judicial, a dados e comunicações realizados por meios eletrônicos, como mensagens em aplicativos de internet, quais sejam WhatsApp, Telegram, Instagram, e-mails, registros de navegação, logs de acesso ou informações armazenadas em servidores e dispositivos digitais.

Sua regulamentação encontra-se primordialmente na Lei nº 12.965/2014, denominada Marco Civil da Internet, que estabelece, em seu artigo 7º, os princípios de proteção à

privacidade e à inviolabilidade das comunicações digitais, condicionando o acesso a esses dados à ordem judicial fundamentada.

Adicionalmente, o Código de Processo Penal (Lei nº 3.689/1941) e, em menor medida, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) complementam o arcabouço normativo, especialmente no que tange à proteção de dados pessoais e à necessidade de justificativa para a medida.

O sigilo telemático pode envolver tanto o acesso a conteúdo pretéritos, mensagens arquivadas, quanto o monitoramento em tempo real, sendo frequentemente utilizada em investigações de crimes cibernéticos, como fraudes eletrônicas, divulgação de conteúdo ilícito ou tráfico de informações sensíveis.

O procedimento envolve, em regra, a solicitação de dados a provedores de serviços de internet ou empresas de tecnologia, que devem cumprir as ordens judiciais sob pena de sanções.

Por outro lado, Quito (2022, p. 183) afirma que a quebra de sigilo telefônico consiste na interceptação de comunicações realizadas por meio da rede de telefonia, incluindo ligações telefônicas e mensagens SMS, ou no acesso a registros de chamadas, como números discados, horários e duração das ligações.

Esta medida é regulada pela Lei nº 9.296/1996, que estabelece requisitos estritos para sua aplicação, como a demonstração de indispensabilidade para a investigação de crimes com pena privativa de liberdade superior a dois anos e a inexistência de outros meios para obtenção da prova.

A interceptação telefônica, em sua forma mais comum, é prospectiva, envolvendo o monitoramento em tempo real das comunicações, com prazo inicial de 15 dias, renovável por igual período, conforme no artigo 8-A, § 3º da lei 9.296/1996.

De acordo com o entendimento de Drakoulakis (2022, p. 32), o acesso a registros de chamadas, também conhecido como quebra de sigilo de dados telefônicos, pode ser retroativo, permitindo a análise de comunicações passadas. Este procedimento é operacionalizado por meio de operadoras de telefonia, que fornecem os dados ou realizam a interceptação conforme determinado judicialmente.

Esta determinação judicial é consolidada no entendimento jurisprudencial, ao qual julgou o Agravo regimental da reclamação 19464, julgado pela Segunda Turma do Supremo Tribunal Federal (STF) em 10 de outubro de 2020, sob a relatoria do Ministro Dias Toffoli.

A ementa do acórdão destaca a inadmissibilidade do afastamento do sigilo de dados telefônicos de jornalistas e empresas de comunicação, enfatizando a importância da

inviolabilidade do sigilo da fonte, conforme previsto no artigo 5º, inciso XIV, da Constituição Federal.

O julgamento analisou a imputação do artigo 10 da Lei nº 9.296/96, que trata da quebra de segredo de justiça sem autorização judicial. A decisão esclareceu que o crime de quebra de sigilo, na modalidade de revelação, é um crime próprio, aplicável apenas a quem tem legítimo acesso ao procedimento de interceptação telefônica, o que não se aplica a jornalistas.

A ausência de aderência inequívoca entre o ato reclamado e a decisão paradigma da ADPF nº 130/DF foi outro ponto central do julgamento. O Supremo Tribunal Federal entendeu que a garantia do sigilo da fonte jornalística não comporta exceções, sendo vedada a quebra de sigilo telefônico de jornalistas ou empresas jornalísticas para apurar vazamentos de informações sigilosas. Os dados obtidos por meio da quebra foram considerados prova ilícita, nos termos do artigo 5º, inciso LVI, da Constituição Federal e do artigo 157 do Código de Processo Penal

A decisão culminou na concessão de habeas corpus de ofício, determinando o trancamento do inquérito policial e a inutilização dos dados obtidos, reforçando a proteção à liberdade de imprensa e ao sigilo das fontes jornalísticas. Veja-se:

> EMENTA AGRAVO REGIMENTAL NA RECLAMAÇÃO. ADPF Nº 130/DF. DIREITO CONSTITUCIONAL E DIREITO PENAL. INQUÉRITO POLICIAL. IMPUTAÇÃO DO ART. 10 DA LEI Nº 9.296/96. AFASTAMENTO DO SIGILO DE DADOS TELEFÔNICOS DE JORNALISTA E DE EMPRESA QUE EDITA PERIÓDICO. SIGILO DA FONTE (ART. 5º, XIV, CF). INEXISTÊNCIA DA EXIGIDA ADERÊNCIA INEQUÍVOCA ENTRE O OBJETO DO ATO RECLAMADO E O CONTEÚDO DA DECISÃO PARADIGMA. INADMISSIBILIDADE DA RECLAMAÇÃO. PRECEDENTES. NÃO PROVIMENTO DO AGRAVO REGIMENTAL. CONSTRANGIMENTO ILEGAL FLAGRANTE CONFIGURADO. HIPÓTESE DE CONCESSÃO DE HABEAS CORPUS DE OFÍCIO. Quebra de segredo de justiça sem autorização judicial (art. 10, segunda parte, da Lei nº 9.296/96) (STF – Rcl 19464 AgR, Relator: Min. DIAS TOFFOLI, Segunda Turma, julgado em 10/10/2020, DJe-291, divulgado em 11/12/2020, publicado em 14/12/2020).

Além disso, nas lições de Grisi Sakamoto (2023, p.45), as diferenciações entre as duas vertentes são significativas, pois enquanto a quebra de sigilo telemático abrange uma ampla gama de dados digitais, incluindo conteúdo armazenados e metadados, como registros de conexão e geolocalização, a quebra de sigilo telefônico limita-se às comunicações realizadas pela infraestrutura de telefonia, excluindo, por exemplo, mensagens trocadas por aplicativos que utilizam a internet.

A regulamentação da quebra telemática é mais recente e reflete o avanço das tecnologias digitais, enquanto a interceptação telefônica possui um arcabouço normativo mais consolidado, porém restrito ao âmbito das comunicações tradicionais.

Além disso, a quebra de sigilo telemático pode ser aplicada a uma gama mais ampla de ilícitos, especialmente aqueles praticados no ambiente virtual, ao passo que a quebra de sigilo telefônico é condicionada a crimes de maior gravidade, conforme exigência da Lei nº 9.296/1996. Ambas, contudo, exigem ordem judicial fundamentada, com demonstração da necessidade e proporcionalidade da medida, a fim de resguardar os direitos fundamentais à privacidade e à intimidade.

Em síntese, a quebra de sigilo telemático e a quebra de sigilo telefônico, embora compartilhem a finalidade de auxiliar na produção de provas em investigações criminais, diferem significativamente em seus objetos, escopos e regulamentações. A primeira adapta-se ao contexto das comunicações digitais, com maior flexibilidade e amplitude, enquanto a segunda permanece restrita às comunicações telefônicas, com requisitos legais mais rigorosos.

A correta aplicação de ambas as medidas exige do julgador a observância dos princípios constitucionais e legais, garantindo o equilíbrio entre a eficácia da persecução penal e a proteção dos direitos fundamentais do cidadão.

2.2.7 Meios de provas e meios de obtenção de provas

Os meios de prova, como ensina Badaró (2017, p.495) são instrumentos utilizados para trazer ao processo elementos que auxiliem o julgador a compreender a verdade dos fatos, distinguem-se dos meios de obtenção de prova, que são os procedimentos para coletar fontes ou elementos probatórios.

A eficácia de medidas como busca e apreensão e interceptação telefônica depende do inesperado, ou seja, do desconhecimento do investigado sobre a medida. Por exemplo, a interceptação telefônica perderia sua utilidade caso o alvo soubesse que suas comunicações estão sendo monitoradas. Isso porque, conforme afirma o doutrinador Rossini (2004, p. 159), obtenção de prova são caminhos para chegar-se à prova.

Contudo, mesmo com o caráter sigiloso, as provas obtidas devem ser submetidas ao princípio do contraditório, permitindo que o réu se defenda das evidências colhidas.

Sidi (2016, p.231) indica que em relação à quebra de sigilo telemático, a classificação das provas pode ser dividida em duas perspectivas:

> Há duas concepções de prova atípica: a restritiva e a ampliativa. Segundo a primeira, prova atípica é aquela que não nominada em lei, ou seja, que não conta com nenhuma

> previsão ou menção na legislação. Já na concepção ampliativa, prova atípica é a que não conta com nenhuma menção ou nominação em lei, mas também é a que é nominada na lei, porém sem previsão de procedimento probatório.

Além disso, conforme o autor, as interceptações telefônicas e telemáticas passaram por três fases distintas ao longo do tempo. Antes da Constituição de 1988, eram consideradas provas atípicas em ambas as concepções, devido à ausência de regulamentação.

Entre a promulgação da Constituição de 1988 e a entrada em vigor da Lei nº 9.296/1996, pela visão restritiva, as interceptações passaram a ser consideradas provas típicas. Entretanto, na perspectiva ampliativa, continuavam atípicas por falta de regulamentação do procedimento legal.

Após a promulgação da Lei nº 9.296/1996, as interceptações foram reconhecidas como provas típicas em ambas as perspectivas, já que a legislação passou a estabelecer normas claras para a sua utilização.

Tanto a busca e apreensão, prevista no Código de Processo Penal, quanto a interceptação telefônica, regulamentada pela Lei nº 9.296/1996, são medidas cautelares utilizadas para a obtenção de provas. Afirma Sidi (2016, p.232) que o material obtido por meio dessas medidas é considerado meio de prova e serve para fundamentar o processo judicial.

De acordo com Avelar (2023, p.92) os meios de prova constituem instrumentos indispensáveis para a formação do convencimento do magistrado, permitindo a obtenção de elementos que elucidam a verdade real dos fatos controvertidos no processo penal.

Conforme previsto no ordenamento jurídico brasileiro, o Código de Processo Penal, instituído pelo Decreto-Lei nº 3.689/1941, apresenta um rol exemplificativo de meios de prova essenciais à instrução criminal. Entre os meios destacam-se o exame de corpo de delito e as perícias, regulamentados nos artigos 158 a 184, que permitem a análise técnica de vestígios relacionados ao fato investigado.

A confissão, tratada nos artigos 197 a 200, consiste em declaração espontânea do acusado que admite a prática delitiva. O depoimento do ofendido, previsto no artigo 201, assim como o testemunho, artigos 202 a 225, oferecem relatos diretos ou indiretos que podem corroborar ou confirmar versões apresentadas.

Adicionalmente, o Código de Processo Penal disciplina procedimentos como o reconhecimento de pessoas ou objetos em seus artigos 226 a 228 e a acareação nos artigos 229 e 230, meios que visam dirimir contradições entre depoimentos.

Os documentos, artigos 231 a 238 e os indícios. artigo 239, também são reconhecidos como valiosos para a prova, assim como a busca e apreensão, artigos 240 a 250, medida cautelar que permite a obtenção de provas indispensáveis ao esclarecimento da verdade.

A jurisprudência e a doutrina reforçam a importância desses meios como ferramentas legítimas para a formação da convicção do juiz, respeitados os princípios do contraditório e da ampla defesa, além dos direitos fundamentais do acusado.

Nesse contexto, Prado (2017, p. 235) destaca que os meios de prova não apenas instruem o processo, mas garantem a efetividade da prestação jurisdicional, embasando decisões judiciais que respeitem a legalidade e a justiça.

No processo penal, é essencial que a prova dos fatos seja obtida de forma clara e eficaz já nas fases de inquérito e instrução, sem depender exclusivamente da confissão do arguido, a qual pode ser retratada em juízo.

Assim, quanto ao meio de obtenção de prova, Greco (2020, p. 64) recomenda que, durante o primeiro interrogatório judicial, inquirido no artigo 141 do Código de Processo Penal, as declarações do arguido sejam acompanhadas de outros elementos probatórios, como documentos, objetos apreendidos, depoimentos e relatórios, permitindo seu confronto com os indícios, o que fortalece o valor probatório nos termos dos artigos 355.º e 357.º do referido código.

Quanto à prova testemunhal, afirma o doutrinador, que na ausência de testemunhas diretas dos fatos, é aconselhável recorrer a testemunhos de natureza policial resultantes de diligências externas, como visitas aos locais dos fatos.

Por fim, quanto à prova documental, destaca Greco (2020, p. 86) a utilidade de fotografar o arguido no momento da detenção ou início da investigação, a fim de auxiliar na sua posterior identificação em julgamento, dada a frequente alteração de características físicas entre os fatos e a audiência.

3- NÍVEIS DE PROTEÇÃO JURÍDICA NA QUEBRA DE SIGILO TELEMÁTICO

Como se compreende a partir do panorama anteriormente traçado, os mecanismos de quebra de sigilo telemático distinguem-se em função da natureza das informações cujo sigilo é afastado, o que acarreta limitação a diferentes garantias constitucionais, em maior ou menor grau.

Ao se considerar uma escala decrescente, Quito (2022, p.180) afirma que para avaliar o grau de restrição às garantias constitucionais impostas por diferentes formas de quebra de sigilo, iniciaria, inevitavelmente, pelas interceptações telemáticas e pelas violações de comunicações armazenadas, que, ocupam o mesmo nível de impacto, como será abordado adiante.

Em seguida, viriam as apreensões de conteúdo armazenados que não se relacionam diretamente ao conteúdo humano de comunicações, estas, dependendo da quantidade e da natureza das informações obtidas, podem, em certos casos, se equiparar às primeiras. Posteriormente, inclui-se o acesso a metadados e, por fim, as quebras de dados cadastrais.

Nesse contexto, Sidi (2016, p. 295) analisa as interceptações telegráficas e telemáticas, destacando o princípio da proporcionalidade no tratamento de diferentes categorias de dados pessoais, sendo os dados de conteúdo humano aqueles com maior expectativa de proteção. De acordo com o autor, os dados de tráfego ocupam o nível mais alto de proteção, enquanto os dados cadastrais estão no nível mais baixo.

O artigo 5º, inciso X, da Constituição Federal estabelece uma proteção geral à intimidade e à vida privada. Já o inciso XII oferece uma tutela adicional, abrangendo, além da intimidade, a liberdade de expressão do pensamento. Por essa razão, as comunicações telemáticas posicionam-se no topo da escala de proteção mencionada anteriormente.

Conforme discutido no item 2.1, desde a promulgação da Constituição de 1988, intensos debates surgiram sobre a constitucionalidade das interceptações telemáticas. A interpretação predominante, tanto na doutrina quanto na jurisprudência, fundamenta-se no artigo 5º, inciso XII, da Constituição.

Ferraz Jr. (2018, p. 148) argumenta que o sigilo constitucionalmente garantido protege o fluxo da comunicação, e não o conteúdo em si, assegurando a liberdade de comunicação sem interferência de terceiros.

Assim, o que violaria essa liberdade seria a intrusão de terceiros em uma comunicação privada, permitindo que informações destinadas a permanecerem entre os interlocutores sejam acessadas por outros.

Essa perspectiva diferencia o sigilo da comunicação da inviolabilidade do conteúdo comunicado. A comunicação privada, portanto, é o bem jurídico protegido, vedando-se a intervenção de terceiros alheios à relação comunicativa. Este entendimento tem sido refletido na jurisprudência brasileira.

No julgamento do Recurso Extraordinário (RE) 418.416/SC, o Supremo Tribunal Federal (STF), sob relatoria do Ministro Sepúlveda Pertence, reforçou que a Constituição protege o fluxo de comunicação de dados, e não os dados em si.

Assim, a apreensão de suportes físicos contendo dados digitais não seria inconstitucional, desde que realizada com autorização judicial. A ementa do julgamento destaca:

> [...] . 2. Na espécie, ao contrário, não se questiona que a apreensão dos computadores da empresa do recorrente se fez regularmente, na conformidade e em cumprimento de mandado judicial. 3. Não há violação do art . 5º. XII, da Constituição que, conforme se acentuou na sentença, não se aplica ao caso, pois não houve "quebra de sigilo das comunicações de dados , mas sim apreensão de base física na qual se encontravam (interceptação das comunicações) os dados, mediante prévia e fundamentada decisão judicial". 4. A proteção a que se refere o art . 5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador (STF - RE: 418416 SC, Relator.: Min. SEPÚLVEDA PERTENCE, Data de Julgamento: 10/05/2006, Tribunal Pleno, Data de Publicação: DJ 19-12-2006 PP-00037 EMENT VOL-02261-06 PP-01233) (grifo nosso).

Embora há de se considerar que o artigo 5º, XII, da Constituição Federal distingue dois blocos, de um lado as comunicações por carta e telegrama e, de outro, as comunicações de dados e telefônicas, todavia, a exceção constitucional estaria relacionada a interceptação telefônica.

No mesmo sentido, Ferraz Jr. (2018, p.45) concluiu que os fluxos de comunicação são sempre invioláveis, conquanto possam ser apreendidos os resultados comunicações já realizadas e a exceção à regra de inviolabilidade do fluxo, prevista na parte final do artigo 5º,

XII, diz respeito unicamente às comunicações telefônicas, as quais, por sua natureza, não deixam registros.

A instantaneidade dos contatos telefônicos justificaria, portanto, a intervenção do Estado no próprio processo de comunicação para deixar fluxos e copia-los, viabilizando a colheita de provas para as investigações e processos criminais.

Ao reconhecer a constitucionalidade do artigo 1º, parágrafo único, da Lei nº 9.296/1996, Grisi Sakamoto (2023, p. 47) destaca que os tribunais brasileiros passaram a admitir, para fins penais, a possibilidade de intromissão de agentes estatais também nas comunicações telemáticas.

Contudo, o autor ainda destaca que se deve obedecer aos mesmos critérios de proporcionalidade exigidos para a interceptação telefônica, quais sejam: adequação, necessidade e proporcionalidade em sentido estrito.

Além disso, a medida está sujeita à limitação temporal de quinze dias, conforme disposto no artigo 5º da Lei nº 9.296/1996, sendo esse prazo prorrogável mediante decisão judicial devidamente fundamentada, desde que demonstrada a real necessidade da continuidade da medida.

Conforme aponta Khedi (2008, p. 242), as comunicações armazenadas digitalmente, embora não estejam em trânsito, continuam amparadas pela proteção constitucional do sigilo, exigindo autorização judicial para acesso, sob pena de ilicitude da prova.

Com isso, as investigações criminais em relação às quebras de sigilo de comunicações telemáticas não se restringem ao monitoramento futuro do fluxo de mensagens, recaindo, frequentemente, sobre o conteúdo de comunicações armazenadas em caixas de mensagens, o que pode equivaler a anos de conversas arquivadas, mas ainda assim resguardadas do conhecimento de terceiros.

Conforme analisa Sidi (2016, p.67), os provedores de e-mail servem-se, na atualidade, de tecnologia imap (internet, mensagem, acesso, protocolo) que permite aos usuários manter com as empresas a totalidade de seus e-mails enviados, recebidos e rascunhos para acessá-los de qualquer lugar e de qualquer dispositivo.

Por conta das características dessa tecnologia, na prática, a totalidade das mensagens podem corresponder a muitos anos, quase décadas de mensagens trocadas, que acabam tendo seus sigilos levantados.

Por mais que a observância aos subprincípios da proporcionalidade fosse de rigor na tomada de qualquer decisão que importe restrição a direitos fundamentais, constata-se, na

prática, uma tendência à flexibilização das comunicações armazenadas sob a justificativa, que, no texto da lei, não há restrições a essa modalidade de quebra.

Não há dúvida de que medidas desse tipo acarretam profunda violação ao sigilo das comunicações e à intimidade, afrontando claramente o postulado da proporcionalidade.

A ausência de limitação temporal na Lei nº 12.965/2014 (Marco Civil da Internet) é causa de evidência excessiva no meio empregado da quebra de sigilo telemático para a consecução do fim da investigação de fato determinado e limitação no tempo.

Esse excesso do fim foi declarado pelo Supremo Tribunal de Justiça, no julgamento do Habeas Corpus nº 315.220/RS, em setembro de 2015, quando a 6ª Turma discutiu a legalidade de quebra de sigilo de e-mails armazenados no período compreendido entre 2004 e 2014, por indivíduo investigado na Operação Revelação, observa-se:

> PROCESSUAL PENAL. HABEAS CORPUS. OPERAÇÃO REVELAÇÃO. CORRUPÇÃO ATIVA. MEDIDAS CAUTELARES DETERMINADAS. AFASTAMENTO DE SIGILO DE CORREIO ELETRÔNICO. DURAÇÃO DA CONSTRIÇÃO. PRAZO: DE 2004 A 2014. FUNDAMENTAÇÃO PARA A QUEBRA DO SIGILO DO E-MAIL NO PERÍODO. AUSÊNCIA. PRINCÍPIO DA PROPORCIONALIDADE. NÃO OBSERVÂNCIA. OFENSA ÀS GARANTIAS CONSTITUCIONAIS. FLAGRANTE ILEGALIDADE. EXISTÊNCIA. ORDEM CONCEDIDA. 1. A quebra do sigilo do correio eletrônico somente pode ser decretada, elidindo a proteção ao direito, diante dos requisitos próprios de cautelaridade que a justifiquem idoneamente, desaguando em um quadro de imprescindibilidade da providência. (STJ - HC: 315220 RS 2015/0019757-0, Relator.: Ministra MARIA THEREZA DE ASSIS MOURA, Data de Publicação: DJ 06/02/2015) (grifo nosso).

A relatora, Ministra Maria Thereza de Assis Moura, considerou que não havia proporcionalidade, pois não demonstrou a imprescindibilidade da quebra proporcional das mensagens de correio eletrônico pelo exorbitante período de dez anos. Embora não unânime o julgamento, o Superior Tribunal de Justiça acabou por conceder a ordem para anular a prova colhida.

Entretanto, a assimetria entre as interceptações telemáticas e as quebras temporais de comunicações armazenadas vai além do que foi tratado pela medida, pois o período que foi tratado ao longo do tempo.

Ao estabelecer que a execução criminal, o artigo 5º, XII, da Constituição Federal observou critério de proporcionalidade em sentido estrito, reforçado pelo artigo 2º, III, da Lei nº 9.296/1996, no qual se previu que apenas a persecução de crimes objetivamente considerados

mais graves pelo legislador, sendo os crimes punidos com reclusão, justifica a restrição excepcional ao sigilo.

Como observa Prado (2017, p. 351), não existe distinção ontológica entre as modalidades de pena privativa de liberdade, de modo que "a diferença entre reclusão e detenção é meramente quantitativa, fundada basicamente na maior gravidade da primeira".

Além disso, Greco (2020, p. 97), pondera que a limitação imposta pelo artigo 2°, III da Lei nº 9.296/1996 quanto à natureza do crime objeto de persecução criminal é falha. Isso porque, se há certo exagero em se admitir interceptações para todos os crimes de reclusão, por outro lado a investigação de crimes de injúria e ameaça praticados por meios eletrônicos pode depender de interceptações telemáticas para viabilizar a formação do conjunto probatório. Assim, argumenta o autor que o melhor seria que a lei tivesse criado um rol taxativo de crimes para os quais as interceptações seriam permitidas.

A redação do Marco Civil da Internet, por sua vagueza, acaba por permitir que extensos registros de crimes punidos com detenção, logo reputadas investigações e processos de crimes punidos com detenção, reputados menos graves, muitos dos quais sequer permitiriam a propositura de ações penais, porque suscetíveis de transação penal ou de suspensão condicional do processo.

Do mesmo modo, permite que extensos períodos de comunicações passadas sejam acessados para a instrução de processos civis, o que é de todo incompatível com a finalidade antevista no artigo 5º, XII, da Constituição Federal.

Sidi (2016, p. 301), esclarece que, do ponto de vista tecnológico, nem mesmo seria possível distinguir as mensagens em trânsito daquelas armazenadas, dado que o armazenamento é um estágio obrigatório da transmissão de e-mails, que são armazenados em diversos computadores entre o momento em que o remetente escreve a mensagem e o destinatário a recebe.

Enfim, o tratamento legal dispensado ao acesso às comunicações armazenadas na Lei nº 12.965/2014 cria o seguinte paradoxo: enquanto em trafego, as mensagens trocadas são protegidas com rigor, no instante seguinte ao seu armazenamento, momento esse que sequer pode ser precisado, o rigor desaparece, viabilizando acesso praticamente irrestrito aos registros de conteúdos comunicados, desde que haja, para tanto, autorização judicial.

4- CONSIDERAÇÕES FINAIS

Conforme demonstrado, qualquer tentativa de harmonizar o tratamento jurídico conferido às comunicações telemáticas em fluxo com aquelas armazenadas, depende do reconhecimento de que, todas as formas de comunicação telemática estão abrangidas pela proteção constitucional prevista no artigo 5º, inciso XII, da Constituição Federal.

Nesse sentido, Barroso (2019, p. 518) destaca que a proteção constitucional do sigilo das comunicações deve alcançar tanto as mensagens em trânsito quanto aquelas armazenadas, garantindo a privacidade e a intimidade dos usuários frente às novas tecnologias.

A fim de alcançar amparo jurídico, qualquer tentativa de uniformizar esse tratamento passará, necessariamente, também pela promoção de alterações legislativas visando instituir, seja no Marco Civil da Internet, seja em outro diploma legal, um disciplinamento próprio às quebras de sigilo de comunicações telemáticas armazenadas.

Para que haja observância ao sigilo das comunicações como disposto no artigo 5º, XII, da Constituição Federal, a regulamentação deverá prever, em primeiro lugar, que as quebras de sigilo de comunicações armazenadas terão finalidade processual penal a depender da existência de indícios razoáveis de autoria ou participação no crime investigado.

Deve-se condicionar as quebras de sigilo de comunicações telemáticas pretéritas à demonstração da imprescindibilidade do meio de obtenção de prova. Como ressalta Fares (2019, p. 34), as medidas devem observar os mesmos critérios de proporcionalidade exigidos para a interceptação telefônica, quais sejam: adequação, necessidade e proporcionalidade em sentido estrito.

Nesse contexto, o acesso a dados armazenados deve ser delimitado temporalmente, conforme os fatos investigados, evitando autorizações amplas e desproporcionais, o que garante maior segurança jurídica e respeito aos direitos fundamentais.

De igual modo, Sidi (2016, p. 62) observa que as comunicações telemáticas armazenadas, embora não estejam em trânsito, continuam protegidas constitucionalmente,

sendo necessário que o acesso se dê mediante decisão judicial fundamentada, sob pena de ilicitude da prova.

A fim de evitar que o meio empregado a quebra de sigilo telemático se dissocie do fim almejado, investigação criminal, entende-se, como aponta Fares (2019, p. 31), que a lei deve conter critérios objetivos e claros para aplicação do princípio da proporcionalidade, como já se verifica na Lei nº 9.296/1996, que disciplina a interceptação de comunicações, impondo limites legais, controle judicial e fundamentação rigorosa.

O desenvolvimento tecnológico alterou significativamente a maneira como nos comunicamos e armazenamos informações pessoais, impactando diretamente o âmbito do processo penal.

As investigações criminais e a constituição de provas em processos judiciais têm recorrido cada vez mais a recursos digitais para obtenção de evidências.

Contudo, a legislação processual penal não evoluiu na mesma velocidade, resultando em lacunas normativas preenchidas por decisões judiciais. Essas decisões, muitas vezes, carecem de padronização e limites claros, o que pode gerar abusos na supervisão estatal sobre as atividades digitais dos indivíduos.

O termo quebra de sigilo telemático é frequentemente utilizado para descrever métodos de obtenção de provas, que envolvem o acesso a informações sigilosas de diferentes naturezas no contexto de investigações criminais.

Dependendo do tipo de informação acessada, cada forma de quebra de sigilo impacta garantias fundamentais em diferentes intensidades.

As principais modalidades de quebra de sigilo digital no processo penal incluem: interceptação de comunicações telemáticas, acesso a comunicações armazenadas, apreensão de conteúdos distintos das comunicações humanas, obtenção de metadados e acesso a informações cadastrais.

Entre essas modalidades, as comunicações telemáticas recebem maior proteção constitucional, conforme estabelecido no artigo 5º, inciso XII, da Constituição Federal, que salvaguarda a privacidade e a liberdade de expressão.

Apesar de parte da doutrina e da jurisprudência ainda interpretar que a proteção constitucional prevista no artigo 5º, inciso XII, da Constituição Federal se aplica apenas ao tráfego das comunicações, ou seja, às comunicações em curso, essa leitura mostra-se defasada frente à realidade tecnológica atual.

Esta interpretação gera uma disparidade na tutela conferida às comunicações em tempo real e àquelas armazenadas, resultando em menor proteção às mensagens já arquivadas.

Contudo, é importante destacar que o sigilo constitucional abrange tanto as comunicações em curso quanto as comunicações humanas armazenadas, independentemente do seu estado de transmissão.

A proteção, no entanto, encontra obstáculos quando se trata de conteúdos em posse de terceiros, como provedores de serviço, o que reforça a necessidade de um marco legal mais claro e específico.

Dessa forma, para garantir segurança jurídica e uniformidade no tratamento das comunicações digitais, é imprescindível que o ordenamento jurídico brasileiro preveja normas específicas para o acesso às comunicações telemáticas armazenadas.

Embora atualmente, o Marco Civil da Internet (Lei nº 12.965/2014) menciona esse tipo de acesso, a regulamentação ainda é genérica e insuficiente, devendo coexistir com o regime próprio das interceptações telemáticas reguladas pela Lei nº 9.296/1996.

O Poder Judiciário, nesse cenário, deve atuar com extrema cautela, garantindo que as autorizações sejam fundamentadas e estritamente proporcionais, considerando a imprescindibilidade das informações para o êxito da investigação criminal.

A pesquisa realizada demonstrou que a norma ainda carece de uma regulamentação adequada para disciplinar o acesso as comunicações armazenadas no contexto penal.

Constata-se assim, que a legislação vigente não contempla as peculiaridades das novas tecnologias, especialmente em relação à natureza e à abrangência das informações digitais acessadas.

Sendo identificado que uma legislação específica deveria, além de regulamentar o acesso, delimitar um rol taxativo de crimes que autorizem a quebra de sigilo telemático, estabelecer critérios objetivos de proporcionalidade e prever uma delimitação temporal clara, como já ocorre com a quebra de sigilo telefônico.

Por fim, conclui-se que o avanço tecnológico, embora traga inúmeros benefícios, impõe o desafio de atualizar o arcabouço jurídico para equilibrar a efetividade das investigações criminais com a proteção dos direitos constitucionais, garantindo segurança jurídica e respeito às garantias individuais no contexto das comunicações telemáticas.

REFERÊNCIAS

ALVES, Daniel de Almeida. **O direito à privacidade, intimidade e proteção de dados dos trabalhadores perante o avanço tecnológico**. 2023. Disponível em: repositorio.sis.puc-campinas.edu.br. Acesso em: 05 jun. 2025.

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. Disponível em: https://lavits.org/wp-content/uploads/2018/04/33-Jacqueline-de-Souza-Abreu-e-Dennys-Antonialli.pdf. Acesso em: 08 jun. 2025.

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**. Diário Oficial da União: seção 1, Brasília, DF, 5 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 9 jun. 2025.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal**. Diário Oficial da União: seção 1, Rio de Janeiro, RJ, 13 out. 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 9 jun. 2025.

BRASIL. **Decreto nº 8.771, de 11 de maio de 2016**. **Regulamenta dispositivos da Lei nº 12.965, de 23 de abril de 2014**. Diário Oficial da União: seção 1, Brasília, DF, 12 maio 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acesso em: 9 jun. 2025.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet**. Diário Oficial da União: seção 1, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 9 jun. 2025.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996. Regula a interceptação de comunicações telefônicas e outros meios de comunicação**. Diário Oficial da União: seção 1, Brasília, DF, 25 jul. 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 10 jun. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l13709.htm. Acesso em: 10 jun. 2025.

BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019.** Diário Oficial da União: seção 1, Brasília, DF, 26 dez. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l13964.htm. Acesso em: 10 jun. 2025.

BRASIL. **Lei nº 13.344, de 6 de outubro de 2016. Dispõe sobre prevenção e repressão ao tráfico interno e internacional de pessoas e sobre medidas de atenção às vítimas**. Diário Oficial da União: seção 1, Brasília, DF, 7 out. 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l13344.htm. Acesso em: 10 jun. 2025.

BRASIL. **Lei nº 6.613, de 16 de dezembro de 1998. Altera dispositivos da Lei nº 6.815, de 19 de agosto de 1980, que dispõe sobre a situação jurídica do estrangeiro no Brasil.** Diário

Oficial da União: seção 1, Brasília, DF, 17 dez. 1998. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l6613.htm. Acesso em: 10 jun. 2025.

BRASIL. **Lei nº 12.683, de 9 de julho de 2012. Altera a Lei nº 9.613, de 3 de março de 1998, para tornar mais eficiente a persecução penal dos crimes de lavagem de dinheiro.** Diário Oficial da União: seção 1, Brasília, DF, 10 jul. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l12683.htm. Acesso em: 10 jun. 2025.

BRASIL. **Lei nº 12.850, de 2 de agosto de 2013. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção de prova, infrações penais correlatas e o procedimento criminal a ser aplicado**. Diário Oficial da União: seção 1, Brasília, DF, 5 ago. 2013. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l12850.htm. Acesso em: 10 jun. 2025.

DRAKOULAKIS, Gessika Christiny. **Acesso à dispositivo telefônico, sem prévia autorização judicial, durante apreensão policial**. Boletim IBCCRIM, v. 30, n. 353, 2022.

DONEDA, Danilo. **Da proteção de dados à proteção da privacidade: uma análise do Marco Civil da Internet.** Revista Brasileira de Direito Civil, Belo Horizonte, v. 4, n. 15,jan./mar. 2015.

FARES, Mohamad Hassan. **Quebra de sigilo telemático**. 2019. Disponível em: https://adelpha-api.mackenzie.br/server/api/core/bitstreams/b6fd45c7-68ff-4f51-972e-314f13d27fc/content. Acesso em: 06 jun. 2025.

FERRAZ JR., Tércio Sampaio. **Direitos fundamentais e processo penal na era digital: doutrina e prática em debate.** São Paulo: InternetLab, 2018. v. 1. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2019/08/InternetLabCongressoII_dupla.pdf. Acesso em: 14 abr.2025.

GRISI SAKAMOTO, Maria Laura. **A constitucionalidade das ordens judiciais de quebra de sigilo telemáticos, de um conjunto não identificado de pessoas, por geolocalização à luz dos direitos à privacidade de intimidade**. Revista Foco (Interdisciplinary Studies Journal), v. 16, n. 1, 2023.

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. Disponível em: https://kehdivieira.com.br/sigilo-das-comunicacoes-e- de-dados/. Acesso em: 05 abr. 2025

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**. RACE – Revista de Administração do Cesmac, v. 4, 2019.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004. Disponível em: https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:livro:2004;000699907. Acesso em: 23 maio 2025.

SAYÃO, Luís Fernando**. Uma outra face dos metadados: informações para a gestão da preservação digital. Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação**, v. 15, n. 30, 2010. Disponível em: https://periodicos.ufsc.br/index.php/eb/article/view/1518-2924.2010v15n30p1/19527. Acesso em: 05 maio 2025.

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. Publicado em: 30 maio 2025. Disponível em: https://jurisprudencia.stf.jus.br/pages/search?base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&queryString=Reclama%C3%0AgR-ED&sort=_score&sortBy=desc. Acesso em: 9 jun. 2025.

STF, **Reclamação nº 19464 SP 8620187-27.2015.1.00.0000**. Relator: Min. Dias Toffoli. Segunda Turma, Julgado em: 10 out. 2020. Publicado em: 14 dez. 2020. Disponível em: https://jurisprudencia.stf.jus.br/pages/search?base=acordaos&pesquisa=Rcl%2019464. Acesso em: 9 jun. 2025.

STF**. Reclamação 418.416/SC**. Relator: Ministro Sepúlveda Pertence. Tribunal Pleno. Julgamento: 10 mai. 2006. Diário da Justiça: seção 1, Brasília, DF, 19 dez. 2006, p. 37. Ementa: vol. 22.261-06, p. 1.233. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur92577/. Acesso em: 10 jun. 2025.

STJ. **Agravo Regimental nos EDcl no RHC n. 157.798/PR.** Relator: Ministro Messod Azulay Neto. Quinta Turma. Julgado em: 12 fev. 2025. Diário da Justiça Eletrônico do STJ, Brasília, DF, Publicado em: 17 fev. 2025. Disponível em: https://scon.stj.jus.br/SCON/pesquisar.jsp?livre=S&operador=e&b=ACOR&tp=T. Acesso em: 10 jun. 2025.

STJ. **Habeas Corpus 315.220/RS.** Relatora: Ministra Maria Thereza de Assis Moura. Sexta Turma. Julgamento: 6 fev. 2015. Diário da Justiça Eletrônico: Brasília, DF, 6 fev. 2015. Disponível em: https://scon.stj.jus.br/SCON/jurisprudencia/doc.jsp?livre=315220&b=ACOR&p=true. Acesso em: 10 jun. 2025.

TOMASEVICIUS FILHO, Eduardo. **Marco Civil da Internet: construção e aplicação.** Juiz de Fora: Editar, 2016. Disponível em: https://www.scielo.br/j/ea/a/n87YsBGnphdHHBSMpCK7zSN. Acesso em: 06 jun. 2025.

VAZ, Denise Provasi. **Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório**. 2012. Tese (Doutorado em Direito) – Faculdade de Direito da Universidade de São Paulo, São Paulo, 2012. Disponível em: https://repositorio.usp.br/item/002281156. Acesso em: 27 maio 2025.

VELLOSO, Fernando. **Informática: conceitos básicos**. Rio de Janeiro: Elsevier Brasil, 2014. p. 56. Disponível em: https://www.academia.edu/35872119/ _B%C3%81SICOS. Acesso em: 21 fev. 2025.