



**PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
ARTIGO CIENTÍFICO**

NATALHA GOMES DE REZENDE SILVA

O IMPACTO DAS REDES SOCIAIS NA PERSECUÇÃO CRIMINAL:
limites constitucionais à obtenção de provas digitais

GOIÂNIA-GO
2026

NATALHA GOMES DE REZENDE SILVA

O IMPACTO DAS REDES SOCIAIS NA PERSECUÇÃO CRIMINAL:

limites constitucionais à obtenção de provas digitais

Artigo Científico apresentado à disciplina
Trabalho de Curso II, da Escola de Direito,
Negócios e Comunicação da Pontifícia
Universidade Católica de Goiás. Prof.(a)
Orientador(a): Dr. Nivaldo dos Santos

GOIÂNIA-GO

2026

O IMPACTO DAS REDES SOCIAIS NA PERSECUÇÃO CRIMINAL:
limites constitucionais à obtenção de provas digitais

Data da Defesa: _____ de _____ de 2026

BANCA EXAMINADORA

Orientadora Prof ^a : Dr. Nivaldo Do Santos	Nota
---	------

Examinador Convidado: Prof ^o Mestre Júlio Anderson Alves Bueno	Nota
---	------

O IMPACTO DAS REDES SOCIAIS NA PERSECUÇÃO CRIMINAL:

limites constitucionais à obtenção de provas digitais

Natalha Gomes de Rezende Silva

RESUMO

O presente artigo científico teve como objetivo analisar o impacto das redes sociais na persecução criminal, abordando como essas plataformas digitais influenciam investigações, produção de provas e decisões judiciais. A pesquisa discute os limites legais e éticos da utilização de conteúdos publicados em redes sociais, bem como os desafios enfrentados pelas autoridades diante da velocidade e alcance da informação digital. A metodologia utilizada é bibliográfica e documental, com análise de jurisprudências do Supremo Tribunal Federal (STF) e do Superior Tribunal de Justiça (STJ), além de doutrina especializada em Direito Processual Penal e Direito Digital. Conclui-se que, embora as redes sociais representem uma ferramenta poderosa para o sistema penal, é necessário garantir o respeito aos direitos fundamentais e à legalidade na obtenção e uso de provas digitais, sendo indispensável a reserva de jurisdição e a observância da cadeia de custódia.

Palavras-chave: Redes sociais; persecução penal; prova digital; cadeia de custódia; direitos fundamentais.

ABSTRACT

This research examines the impact of social media on criminal prosecution, focusing on the constitutional limits regarding the collection and use of digital evidence. The study highlights how the increasing reliance on social networks as sources of information poses challenges to fundamental rights, particularly privacy, due process, and the presumption of innocence. Using a bibliographic and doctrinal methodology, the work analyzes Brazilian constitutional principles, relevant legislation, and judicial precedents from the Federal Supreme Court (STF) and the Superior Court of Justice (STJ) to identify the boundaries of lawful evidence gathering in the digital environment. The findings reveal that, although social media provides valuable tools for criminal investigations, unrestricted access to digital content risks violating constitutional guarantees. Therefore, the study emphasizes the need for clear legal frameworks, the principle of jurisdictional reserve, and strict compliance with the chain of custody to balance the effectiveness of criminal prosecution with the protection of fundamental rights.

Keywords: Social media; criminal prosecution; digital evidence; chain of custody; fundamental rights.

INTRODUÇÃO

A expansão das redes sociais nas últimas décadas transformou de maneira profunda as relações humanas e, por consequência, o próprio cenário da criminalidade e da investigação penal. Plataformas como *Facebook*, *Instagram*, *WhatsApp*, *X* (antigo *Twitter*) e *TikTok* tornaram-se espaços nos quais pessoas compartilham informações, mantêm conversas privadas e, muitas vezes, produzem ou deixam vestígios de atividades ilícitas. Diante desse novo cenário, as autoridades responsáveis pela persecução criminal passaram a utilizar as redes sociais como fonte privilegiada de elementos probatórios.

A utilização de dados digitais oriundos dessas plataformas, contudo, não é isenta de problemas jurídicos. O principal deles reside na tensão entre a eficácia da investigação criminal e a proteção dos direitos fundamentais dos cidadãos. A Constituição Federal de 1988, em seu art. 5º, assegura a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas (inciso X), o sigilo das comunicações (inciso XII) e a inadmissibilidade das provas obtidas por meios ilícitos (inciso LVI). Esses preceitos impõem limites objetivos à atuação estatal na coleta de dados digitais, inclusive aqueles disponíveis ou trocados em redes sociais.

O tema ganha relevância ainda maior diante do crescente uso de técnicas investigativas que incluem o monitoramento de perfis públicos, a requisição de dados cadastrais e de registros de conexão a provedores de internet, a interceptação de comunicações privadas e a cooperação com plataformas estrangeiras. Cada uma dessas práticas suscita discussões sobre sua constitucionalidade e legalidade, especialmente à luz do Marco Civil da Internet (Lei nº 12.965/2014), da Lei Geral de Proteção de Dados Pessoais LGPD (Lei nº 13.709/2018) e do Código de Processo Penal, com as alterações promovidas pelo Pacote Anticrime (Lei nº 13.964/2019).

A questão é ainda mais sensível quando se considera que as provas digitais possuem características intrínsecas que as diferenciam das provas físicas tradicionais: imaterialidade, volatilidade e maleabilidade. Tais atributos exigem do operador do Direito um tratamento metodológico rigoroso, capaz de assegurar a autenticidade e a integridade dos elementos colhidos, sob pena de nulidade processual.

Nesse contexto, o presente artigo tem como objetivo analisar os limites constitucionais à obtenção de provas digitais oriundas das redes sociais no âmbito da persecução criminal. Para tanto, adota-se metodologia de pesquisa bibliográfica e documental, com análise da doutrina jurídica especializada, da legislação pertinente e da jurisprudência do Supremo Tribunal Federal (STF) e do Superior Tribunal de Justiça (STJ). O trabalho está estruturado em três seções principais: a primeira examina a transformação da prova penal no ambiente digital; a segunda analisa a sociedade digital, o conceito de prova digital e os limites constitucionais à sua obtenção; e a terceira discute a interação entre a Lei Geral de Proteção de Dados e o processo penal.

1 REDES SOCIAIS E A TRANSFORMAÇÃO DA PROVA NO PROCESSO PENAL

A era digital alterou profundamente a dinâmica probatória no Direito Processual Penal brasileiro. As redes sociais deixaram de ser meros espaços de interação social para se tornarem vastos repositórios de vestígios digitais, exigindo uma releitura de institutos clássicos sob a ótica da cadeia de custódia e do direito fundamental à não autoincriminação. Essa transformação impõe ao sistema jurídico a necessidade de adaptar categorias tradicionais como documento, indício e prova ao ambiente digital, cujas especificidades técnicas impactam diretamente a validade e a admissibilidade dos elementos probatórios.

A natureza da prova digital é marcada por características que a distinguem fundamentalmente das provas físicas. Diferentemente de um documento em papel ou de um objeto apreendido em uma busca e apreensão, a prova colhida em redes sociais como postagens, mensagens diretas, registros de localização e metadados é marcada pela volatilidade e pela facilidade de alteração. Isso exige que o operador

do Direito não apenas apresente o conteúdo digital, mas garanta, por meios técnicos adequados, a integridade do suporte e a rastreabilidade da coleta.

1.1 AUTENTICIDADE: GARANTIA DE QUE A PROVA PROVÉM DA FONTE ALEGADA

No que diz respeito à evidência digital, um dos pré-requisitos mais relevantes para sua admissibilidade em processos criminais é a autenticação da mesma, uma vez que isso representa uma garantia de que o rastro digital apresentado em juízo é, de fato, idêntico ao que foi gerado por um dos autores do crime ou por testemunhas de um evento. Como os dados digitais podem ser alterados com facilidade, inclusive às vezes de um modo que não é visível ao olho humano desarmado, a autenticidade atua como uma salvaguarda contra a apresentação de evidências deturpadas ou que já não sejam adequadamente representativas.

Sem informações de respaldo autênticas, todo o conjunto probatório seria considerado irrelevante ou não suficientemente confiável para convencer um júri, e uma pessoa inocente poderia sair livre ou um lado oposto culpado poderia ter sido condenado. É por isso que, na modernidade, a doutrina do processo penal teria dedicado cada vez mais atenção a essa questão. Como adverte Lopes Jr. (2023, p. 542):

No processo penal, a autenticidade não é apenas uma questão de autoria, mas de integridade da fonte. A prova deve ser rastreável desde o momento em que é identificada até o seu desentranhamento ou valoração em sentença, sob pena de nulidade por quebra da cadeia de custódia.

A jurisprudência brasileira, especialmente no âmbito do STJ, tem sido rigorosa quanto à autenticidade de mensagens extraídas de aplicativos de comunicação. O tribunal firmou entendimento de que o simples *print screen* de conversas obtidas pelo *WhatsApp Web* não é suficiente para garantir a autenticidade da prova, pois não preserva os metadados nem a sequência lógica irrefutável dos diálogos. Consoante o entendimento consolidado na Sexta Turma do STJ, no julgamento do RHC

133.430/PE, mensagens obtidas por meio do espelhamento do *WhatsApp Web* não podem ser admitidas como prova se não houver demonstração da autenticidade e da integridade da cadeia de custódia, dada a possibilidade de exclusão remota de mensagens sem deixar vestígios.

Para garantir a autenticidade no processo penal, a ciência forense digital recomenda a utilização de, ao menos, três critérios técnicos: (a) identificação de endereços IP, para vincular o dispositivo à autoria; (b) verificação de *hashes* criptográficos, para garantir que o arquivo analisado é idêntico ao coletado na fonte original; e (c) extração e análise de metadados de autoria, que identificam o *software*, o usuário criador e o histórico de modificações do arquivo. A ausência de qualquer desses elementos fragiliza a cadeia probatória e pode resultar no reconhecimento da nulidade da prova.

1.2 A CADEIA DE CUSTÓDIA (ART. 158-A A 158-F DO CPP)

Com o advento do Pacote Anticrime (Lei nº 13.964/2019), a preservação do histórico da prova tornou-se condição de validade no ordenamento processual penal brasileiro. Os arts. 158-A a 158-F do Código de Processo Penal passaram a disciplinar expressamente a cadeia de custódia, definindo-a como o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, com o objetivo de rastrear sua posse e manuseio desde o reconhecimento até o descarte.

No caso das provas digitais oriundas de redes sociais, a simples captura de tela (*print screen*) tem sido sistematicamente questionada pelos tribunais superiores, precisamente porque esse método não preserva os metadados associados às mensagens nem impede a manipulação posterior dos diálogos. A ausência de uma cadeia de custódia adequada pode resultar, conforme o § 1º do art. 158-B do CPP, na inadmissibilidade da prova ou na sua valoração negativa pelo julgador.

A utilização de ferramentas técnicas como o *hash* criptográfico e a lavratura de ata notarial são métodos que conferem maior robustez jurídica ao elemento probatório digital. O *hash* garante que qualquer alteração posterior no arquivo será detectável, pois o valor da função se modifica diante de qualquer mudança no conteúdo. A ata

notarial, por sua vez, confere fé pública ao ato de coleta, tornando-o resistente a impugnações futuras.

Importante distinguir, ainda, as situações de perfis públicos e de comunicações privadas nas redes sociais. Informações acessíveis a qualquer usuário sem restrições de privacidade podem, em regra, ser coletadas pelas autoridades investigativas sem autorização judicial. Já o acesso a mensagens diretas, grupos restritos ou perfis protegidos por configurações de privacidade exige, obrigatoriamente, ordem judicial fundamentada, sob pena de nulidade da prova obtida por violação do sigilo constitucionalmente tutelado.

A transformação da prova penal pelas redes sociais exige que o Direito migre da análise meramente documental para a análise forense computacional. A validade de uma condenação, no ambiente digital, depende menos do que está escrito na tela e mais de como essa informação foi extraída, preservada e apresentada em juízo. A inobservância dessas exigências técnicas e jurídicas compromete não apenas a admissibilidade da prova, mas a legitimidade democrática do próprio processo penal.

1.3 TÉCNICAS INVESTIGATIVAS DIGITAIS E SEUS LIMITES JURÍDICOS

Além da coleta de conteúdos publicados em redes sociais, as autoridades investigativas têm recorrido a técnicas mais sofisticadas de obtenção de provas digitais, cada uma delas sujeita a limites jurídicos específicos. Entre as principais, destacam-se: o monitoramento de perfis públicos; a requisição de dados cadastrais e registros de conexão a provedores de internet; a interceptação telemática de comunicações privadas; a cooperação jurídica internacional com plataformas estrangeiras; e o uso de ferramentas de inteligência artificial para análise de grandes volumes de dados.

O Marco Civil da Internet (Lei nº 12.965/2014) estabelece, em seu art. 22, que as autoridades competentes podem requisitar dados cadastrais de provedores de conexão e de aplicações de internet, desde que observados os requisitos legais e mediante autorização judicial quando se tratar de dados protegidos pelo sigilo. A Lei nº 9.296/1996, por sua vez, disciplina a interceptação de comunicações telefônicas e

telemáticas, condicionando sua realização à existência de indícios razoáveis de autoria ou participação em infração penal, à impossibilidade de produção da prova por outros meios e à existência de crime apenado com reclusão.

A requisição de dados a plataformas estrangeiras como Meta (*Facebook e Instagram*) e *Alphabet* (Google e YouTube) apresenta desafios adicionais, pois essas empresas estão sujeitas às legislações de seus países de origem, o que pode conflitar com as determinações das autoridades brasileiras. O STF, no julgamento da ADI 5.527, firmou entendimento sobre a constitucionalidade da suspensão de serviços de aplicativos de comunicação como medida sancionatória pelo descumprimento de decisões judiciais, evidenciando a complexidade das relações entre soberania estatal e plataformas digitais transnacionais.

2 A SOCIEDADE DIGITAL, A PROVA DIGITAL E OS LIMITES CONSTITUCIONAIS

Nas últimas décadas, a consolidação da internet e a expansão das redes sociais transformaram profundamente as formas de relação, comunicação e compartilhamento de informações entre os indivíduos. Plataformas como Facebook, Instagram, *WhatsApp* e X passaram a funcionar como espaços de interação cotidiana, nos quais dados pessoais, opiniões, registros de atividades e comunicações privadas são constantemente gerados e disponibilizados muitas vezes sem que o próprio usuário tenha plena consciência das implicações jurídicas de sua exposição digital.

Esse cenário inaugura uma nova dimensão da vida social, em que a exposição de informações voluntária ou involuntária ocorre em ambiente digital de difícil controle pelo titular dos dados. Do ponto de vista jurídico, essa transformação impacta diretamente a persecução criminal: a investigação e o processo penal enfrentam um volume crescente de dados digitais que podem servir como elementos probatórios. No entanto, a utilização dessas informações demanda reflexão cuidadosa sobre os limites constitucionais e a proteção dos direitos fundamentais.

2.1 O CONCEITO E AS CARACTERÍSTICAS DA PROVA DIGITAL

A prova digital, também denominada prova eletrônica ou informática, pode ser compreendida como qualquer informação dotada de valor probatório que esteja armazenada ou sendo transmitida por meio de um dispositivo eletrônico. Sua diferença fundamental em relação às provas físicas tradicionais reside no fato de que ela não existe no suporte material (o *hardware*), mas nos dados binários que a constituem dados estes que podem ser copiados, alterados ou destruídos sem deixar rastros aparentes a olho nu.

Segundo Teixeira (2022, p. 85), a prova digital tem natureza desmaterializada:

A prova digital consiste em informações armazenadas ou transmitidas em formato binário (bits), que podem ser acessadas e lidas por meio de sistemas computacionais, possuindo aptidão para demonstrar a veracidade de um fato em juízo.

Assim, o conceito abrange desde *e-mails* e mensagens de aplicativos de comunicação instantânea (como *WhatsApp*, *Telegram* e *Signal*) até logs de acesso a sistemas, metadados ocultos em arquivos de imagem e som, registros de geolocalização e publicações em redes sociais. Três características são centrais para a compreensão jurídica da prova digital.

A imaterialidade indica que a prova existe no campo lógico (software/dados) e não necessariamente no campo físico, o que torna inadequados os tradicionais mecanismos de apreensão material. A volatilidade expressa a facilidade com que os dados podem ser alterados, deletados ou corrompidos se não forem preservados adequadamente por meio de procedimentos técnicos específicos. A maleabilidade, por fim, reflete a possibilidade de manipulação sem deixar vestígios aparentes, o que exige perícia técnica especializada para detectar eventuais adulterações.

Camargo (2021) ressalta que a validade jurídica da prova digital está intrinsecamente ligada à preservação de sua integridade: para que o dado digital seja admitido como prova, deve-se garantir que o conteúdo apresentado em juízo seja idêntico ao extraído

da fonte original, mantendo-se a incolumidade dos *bits*. Qualquer desvio nessa cadeia de integridade compromete a admissibilidade e a valoração do elemento probatório.

2.2 REDES SOCIAIS COMO FONTE DE PROVA NA PERSECUÇÃO CRIMINAL

A utilização de conteúdos de redes sociais como fonte de prova tornou-se prática recorrente e, em muitos casos, determinante em investigações criminais brasileiras. Autoridades policiais e membros do Ministério Público costumam recorrer a conteúdos publicados ou compartilhados nas plataformas para fundamentar acusações, e, em inúmeros casos, os próprios investigados fornecem, de forma voluntária e muitas vezes inconsciente, elementos que indicam autoria ou materialidade de delitos.

São exemplos concretos desse fenômeno: a utilização de fotografias publicadas em redes sociais como prova de ostentação patrimonial incompatível com a renda declarada, em processos de lavagem de dinheiro e tráfico de entorpecentes; o uso de postagens e comentários para demonstrar ameaças, calúnias e injúrias; a coleta de registros de localização para contradizer álibi apresentado pela defesa; e a análise de mensagens trocadas em grupos de *WhatsApp* para identificar a estrutura e o *modus operandi* de organizações criminosas.

Contudo, a coleta e o uso dessas informações não podem ocorrer sem controles jurídicos adequados. A Constituição Federal assegura direitos fundamentais como intimidade, vida privada e sigilo das comunicações, que funcionam como barreiras contra abusos estatais. O desafio central, portanto, é conciliar a eficiência da persecução penal com a observância das garantias constitucionais, de modo a assegurar que o processo penal não se converta em instrumento de opressão ou de devassa indiscriminada na vida privada dos cidadãos.

2.3 A TENSÃO ENTRE EFICIÊNCIA INVESTIGATIVA E GARANTIAS CONSTITUCIONAIS

O processo penal brasileiro é orientado pela busca da verdade real, mas esse objetivo não pode prescindir da proteção dos direitos fundamentais. Há, nesse campo, uma

tensão permanente e estrutural entre a eficiência da investigação criminal que demanda acesso rápido e amplo a dados digitais e as garantias constitucionais que impõem limites à atuação estatal, independentemente da gravidade do crime investigado.

Essa tensão manifesta-se em situações concretas e recorrentes: o acesso a mensagens privadas armazenadas em dispositivos apreendidos sem autorização judicial; o uso de publicações feitas em perfis de acesso público como prova sem observância de qualquer cautela procedimental; a requisição extrajudicial de dados a provedores de internet; e a utilização de técnicas de *data mining* e inteligência artificial para perfilar suspeitos a partir do cruzamento de dados de diversas plataformas digitais.

O STJ, no julgamento do HC 598.051/SP (Rel. Min. Ribeiro Dantas, 2020), estabeleceu marco importante ao fixar que a autorização para a busca e apreensão de dispositivos eletrônicos não implica, automaticamente, autorização para o acesso ao conteúdo desses dispositivos. Segundo o tribunal, o acesso ao conteúdo de aparelhos celulares exige decisão judicial específica e fundamentada, que delimite o escopo da diligência e justifique, à luz do princípio da proporcionalidade, a invasão na esfera privada do investigado.

2.4 PRIVACIDADE, SIGILO DAS COMUNICAÇÕES E RESERVA DE JURISDIÇÃO

No ordenamento jurídico brasileiro, a proteção à privacidade e ao sigilo das comunicações encontra amparo constitucional no art. 5º, incisos X e XII, da Constituição Federal de 1988. No contexto da prova digital, essa proteção ganha novos e mais complexos contornos, uma vez que dispositivos móveis e perfis em redes sociais armazenam aquilo que a doutrina moderna denomina projeção da personalidade do indivíduo um conjunto vasto e íntimo de informações que vai muito além do conteúdo de uma ligação telefônica interceptada.

É fundamental distinguir entre o sigilo das comunicações e a privacidade de dados. O sigilo das comunicações, tutelado pelo inciso XII do art. 5º, refere-se ao fluxo de informações em tempo real mensagens sendo transmitidas no exato momento da

interceptação. A privacidade digital, por sua vez, abrange os dados estáticos já armazenados, como mensagens recebidas e enviadas, fotografias, histórico de localização e registros de atividade, cuja proteção decorre do inciso X do mesmo dispositivo constitucional.

Sobre o tema, Lopes Jr. (2023, p. 612) é categórico ao afirmar:

O acesso a um smartphone sem autorização judicial ou consentimento válido é uma devassa na vida privada que vai muito além de uma simples revista pessoal. Trata-se de um 'contêiner de informações' que exige a proteção do juiz das garantias para que não ocorra uma pesca probatória (fishing expedition).

Para que o sigilo das comunicações digitais seja legitimamente rompido no processo penal, é indispensável a observância da cláusula de reserva de jurisdição. Isso significa que apenas o magistrado competente, mediante decisão devidamente fundamentada e dentro das hipóteses taxativamente previstas em lei como a Lei nº 9.296/1996 para interceptações telemáticas, pode autorizar o acesso aos dados protegidos.

A doutrina e a jurisprudência brasileiras têm incorporado progressivamente a teoria das expectativas de privacidade, oriunda do direito norte-americano, como critério para delimitar o nível de proteção constitucional exigível em cada situação. De acordo com essa teoria, o grau de proteção varia conforme a razoável expectativa de privacidade que o titular dos dados poderia ter em relação ao conteúdo exposto. Dados voluntariamente tornados públicos em perfis abertos comportam proteção menor; já informações compartilhadas em ambientes privados ou semiprivados demandam proteção equivalente à das comunicações privadas tradicionais (Sarlet; Marinoni; Mitidiero, 2022).

2.5 DEVIDO PROCESSO LEGAL, PROPORCIONALIDADE E INADMISSIBILIDADE DAS PROVAS ILÍCITAS

O devido processo legal, previsto no art. 5º, inciso LIV, da Constituição Federal, estabelece que nenhuma pessoa será privada de sua liberdade ou de seus bens sem o devido processo. Esse princípio impõe limites substantivos e procedimentais à atuação estatal, exigindo que a coleta de provas digitais seja realizada de forma legítima, transparente, documentada e proporcional ao fim investigativo perseguido.

O princípio da proporcionalidade, enquanto metanorma de ponderação, exige que as medidas investigativas invasivas sejam: (a) adequadas, ou seja, aptas a alcançar o fim investigativo pretendido; (b) necessárias, vale dizer, inexistindo outros meios menos gravosos para a obtenção da mesma prova; e (c) proporcionais em sentido estrito, de modo que o ganho para a persecução criminal justifique, à luz dos valores constitucionais em jogo, a interferência na esfera privada do investigado.

O inciso LVI do art. 5º da Constituição Federal consagra a inadmissibilidade das provas obtidas por meios ilícitos. Esse dispositivo tem aplicação direta às provas digitais obtidas em violação às garantias constitucionais, conduzindo à sua nulidade e, por força da teoria dos frutos da árvore envenenada (*fruits of the poisonous tree*), à contaminação de todos os elementos probatórios dela derivados. O STF tem aplicado esse entendimento de forma consistente, reconhecendo a ilicitude de provas digitais obtidas sem autorização judicial ou em desrespeito à cadeia de custódia.

3 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E O PROCESSO PENAL

3.1 CONTEXTO HISTÓRICO E FUNDAMENTOS DA PROTEÇÃO DE DADOS NO BRASIL

A proteção de dados pessoais tornou-se uma das grandes questões jurídicas do século XXI, impulsionada pelo vertiginoso avanço tecnológico que transformou o perfilamento, o monitoramento e o direcionamento de indivíduos em práticas rotineiras no âmbito empresarial e estatal. No Brasil, a regulamentação específica sobre privacidade e dados pessoais passou por um longo processo histórico que culminou na aprovação da Lei nº 13.709, de 14 de agosto de 2018 a Lei Geral de Proteção de Dados Pessoais (LGPD).

Até a aprovação da LGPD, o marco jurídico brasileiro tratava a proteção de dados de forma fragmentada, distribuída em estatutos setoriais como o Código de Defesa do Consumidor (Lei nº 8.078/1990), a Lei do Habeas Data (Lei nº 9.507/1997), o Marco Civil da Internet (Lei nº 12.965/2014) e o Decreto nº 8.771/2016. Esse mosaico normativo gerava incerteza jurídica, particularmente para empresas que atuam no ambiente digital, as quais se viam diante de obrigações difusas e, por vezes, contraditórias.

O contexto internacional desempenhou papel determinante no processo legislativo brasileiro. A aprovação do Regulamento Geral sobre a Proteção de Dados (GDPR) pela União Europeia, em abril de 2016, com início de vigência em maio de 2018, intensificou o debate global sobre privacidade e alertou países sem legislação adequada sobre os riscos de exclusão dos fluxos internacionais de dados.

Após quase oito anos de debates parlamentares e consultas públicas, o Congresso Nacional aprovou a LGPD. Com vigência a partir de setembro de 2020 e sanções administrativas aplicáveis desde agosto de 2021, a lei reconhece a proteção de dados pessoais como direito fundamental autônomo posição reforçada pela Emenda Constitucional nº 115/2022, que inseriu essa proteção no rol de direitos fundamentais do art. 5º da Constituição Federal.

3.2 O DIREITO À PRIVACIDADE E À INTIMIDADE COMO LIMITE À OBTENÇÃO DE PROVAS DIGITAIS

O art. 5º, inciso X, da Constituição Federal dispõe que a intimidade, a vida privada, a honra e a imagem das pessoas são invioláveis, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação. Esse dispositivo é um dos principais fundamentos constitucionais que limitam a atuação estatal na coleta de provas digitais em redes sociais, pois exige que qualquer intervenção na vida privada dos cidadãos seja justificada, fundamentada e proporcional.

A doutrina reconhece que o direito à privacidade apresenta diferentes gradações de intensidade, conforme o nível de exposição voluntária do titular dos dados.

Informações deliberadamente tornadas públicas em perfis abertos de redes sociais possuem expectativa de privacidade reduzida, podendo ser coletadas pelos órgãos investigativos sem autorização judicial. Já dados compartilhados em ambientes digitais privados ou semiprivados como grupos fechados de mensagens instantâneas, *stories* com restrição de visualização ou mensagens diretas ostentam expectativa de privacidade elevada, equivalente à das comunicações privadas tradicionais.

Essa distinção, fundamentada na teoria das esferas de privacidade e na teoria das expectativas razoáveis de privacidade (*reasonable expectation of privacy*), tem sido progressivamente incorporada pela jurisprudência dos tribunais superiores brasileiros, orientando o julgamento de casos que envolvem a admissibilidade de provas digitais obtidas em redes sociais. Sarlet, Marinoni e Mitidiero (2022) ressaltam que a aplicação dessa teoria exige do julgador uma análise contextual e casuística, atenta às configurações de privacidade definidas pelo usuário e ao contexto comunicativo em que a informação foi produzida e compartilhada.

O simples fato de uma informação estar disponível em uma rede social não autoriza sua utilização como prova no processo penal. É preciso avaliar as configurações de privacidade definidas pelo usuário, o contexto em que a informação foi divulgada e a expectativa razoável de privacidade que o titular dos dados poderia ter. O descumprimento dessas balizas acarreta a ilicitude da prova e, conseqüentemente, sua inadmissibilidade no processo penal.

3.3 A LGPD NO DIREITO PROCESSUAL PENAL: PROVAS DIGITAIS E DADOS SENSÍVEIS

A LGPD estabelece, em seu art. 4º, inciso III, que não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais. Contudo, essa exclusão não é absoluta: o parágrafo único do mesmo artigo determina que o tratamento de dados nessas hipóteses deverá ser regido por legislação específica, que deverá prever procedimentos e salvaguardas adequados à proteção dos direitos dos titulares.

Na ausência de legislação específica que regule o tratamento de dados pessoais para fins de persecução penal, prevalece um vácuo normativo que abre espaço para práticas potencialmente abusivas. O princípio de segurança da LGPD segundo o qual os dados pessoais devem ser protegidos contra acesso não autorizado, destruição, perda ou alteração indevida guarda relação direta com as exigências da cadeia de custódia no processo penal, impondo que os dados coletados sejam armazenados e tratados com medidas técnicas e administrativas aptas a preservar sua integridade e confidencialidade.

A questão torna-se ainda mais delicada quando envolve dados sensíveis categoria especialmente protegida que inclui dados de saúde, dados genéticos, dados biométricos, origem étnica ou racial, convicção religiosa e vida sexual. O art. 11 da LGPD estabelece regime de tratamento mais restritivo para essa categoria, exigindo fundamento legal específico para seu processamento. No contexto da persecução penal, o uso de dados sensíveis é frequente: coleta de material genético para confronto com vestígios de crime, reconhecimento facial por câmeras de vigilância e acesso a prontuários médicos como fonte de prova.

O uso de sistemas de reconhecimento facial por forças de segurança pública é exemplo paradigmático das tensões entre eficiência investigativa e proteção de direitos fundamentais. Estudos internacionais demonstram que algoritmos de reconhecimento facial apresentam taxas de erro significativamente maiores para pessoas negras e mulheres, o que levanta sérias questões sobre a compatibilidade dessas tecnologias com o princípio da não discriminação da LGPD e com os princípios constitucionais de igualdade e presunção de inocência.

3.4 JURISPRUDÊNCIA DO STF E DO STJ SOBRE PROVAS DIGITAIS EM REDES SOCIAIS

A análise da jurisprudência dos tribunais superiores brasileiros revela uma tendência progressiva de ampliação das garantias constitucionais no campo da prova digital, com especial ênfase na reserva de jurisdição e na exigência de observância da cadeia de custódia.

No âmbito do STF, o julgamento do Recurso Extraordinário nº 1.055.941/SP (Tema 987 da Repercussão Geral, Rel. Min. Gilmar Mendes, 2019) estabeleceu balizas fundamentais para o compartilhamento de dados entre autoridades fiscais e autoridades penais, determinando que o repasse de informações protegidas pelo sigilo fiscal e bancário depende de autorização judicial, sob pena de violação às garantias constitucionais de privacidade e ao devido processo legal.

O STJ, no julgamento do HC 598.051/SP (Rel. Min. Ribeiro Dantas, 2020), firmou tese paradigmática ao decidir que é ilícita a prova obtida mediante acesso ao conteúdo de aparelho celular apreendido sem prévia autorização judicial, ainda que no contexto de prisão em flagrante. O tribunal ressaltou que o celular é um repositório de informações íntimas que supera, em abrangência e profundidade, qualquer outro meio de comunicação anteriormente conhecido, o que justifica o tratamento diferenciado e a exigência de reserva de jurisdição.

No que se refere especificamente às provas obtidas em redes sociais, o STJ tem adotado postura criteriosa quanto à admissibilidade de mensagens extraídas de aplicativos de comunicação. No julgamento do RHC 133.430/PE, a Sexta Turma fixou o entendimento de que conversas obtidas pelo espelhamento do *WhatsApp Web* são inadmissíveis como prova quando não comprovadas a autenticidade e a integridade da cadeia de custódia, em razão da possibilidade de exclusão remota de mensagens sem deixar rastros.

O Habeas Corpus nº 168.052/SP, julgado pelo STF em 2019, abordou a validade de provas digitais obtidas mediante cooperação internacional com plataformas estrangeiras, sinalizando para a necessidade de observância dos tratados internacionais de assistência jurídica mútua (MLAT) e dos procedimentos de homologação judicial como condição de validade dessas provas no processo penal brasileiro.

CONCLUSÃO

O presente artigo teve como objetivo central analisar os limites constitucionais impostos à obtenção de provas digitais em redes sociais no âmbito da persecução criminal. A partir da pesquisa bibliográfica e documental realizada, com exame da doutrina especializada, da legislação vigente e da jurisprudência do Supremo Tribunal Federal e do Superior Tribunal de Justiça, foi possível constatar que a expansão das redes sociais criou um cenário inédito e complexo para a investigação penal, impondo ao ordenamento jurídico brasileiro o desafio de conciliar a eficiência da persecução criminal com a proteção dos direitos fundamentais dos cidadãos.

Verificou-se que a Constituição Federal de 1988 estabelece um sistema robusto de garantias que delimita a atuação estatal no ambiente digital. O direito à intimidade e à vida privada, consagrado no art. 5º, inciso X, o sigilo das comunicações, previsto no inciso XII, e o princípio do devido processo legal, inscrito no inciso LIV, funcionam como barreiras objetivas contra práticas investigativas arbitrárias. Esses preceitos não se restringem ao mundo físico, estendendo-se integralmente às interações digitais, o que impede que a simples disponibilidade de informações em plataformas digitais seja interpretada como autorização implícita para seu uso irrestrito como prova no processo penal.

Constatou-se, ainda, que a prova digital possui características próprias imaterialidade, volatilidade e maleabilidade que exigem do operador do direito um tratamento metodológico diferenciado em relação às provas físicas tradicionais. A cadeia de custódia, disciplinada nos arts. 158-A a 158-F do CPP, com as alterações introduzidas pelo Pacote Anticrime, revelou-se instrumento indispensável para garantir a autenticidade e a integridade dos elementos probatórios colhidos em ambiente digital.

No que diz respeito à distinção entre perfis públicos e comunicações privadas, a pesquisa demonstrou que a teoria das expectativas de privacidade representa um critério adequado para delimitar o nível de proteção constitucional exigível em cada situação. O acesso a mensagens privadas, perfis restritos ou quaisquer dados protegidos por configurações de privacidade do usuário demanda, obrigatoriamente, ordem judicial fundamentada, sob pena de nulidade da prova por violação ao sigilo constitucionalmente tutelado.

A análise da jurisprudência do STF e do STJ revelou uma tendência consolidada de ampliação das garantias no campo da prova digital, com destaque para as decisões que exigem reserva de jurisdição para o acesso ao conteúdo de dispositivos eletrônicos apreendidos e para a quebra do sigilo de comunicações telemáticas.

A LGPD, embora não se aplique diretamente às atividades de persecução penal, impõe, por via reflexa, parâmetros de proteção que influenciam o tratamento de dados pessoais coletados no curso de investigações. A ausência de legislação específica que regule o tratamento de dados para fins penais representa lacuna normativa que deve ser suprida pelo legislador com urgência, à luz das diretrizes constitucionais e da experiência do direito comparado.

Diante do exposto, conclui-se que as redes sociais representam uma ferramenta de inegável valor para a persecução criminal contemporânea, oferecendo elementos probatórios que seriam de difícil ou impossível obtenção por meios tradicionais. No entanto, a utilização dessas plataformas como fonte de prova não pode ocorrer à margem do ordenamento constitucional. A legitimidade da condenação criminal depende não apenas do que foi descoberto, mas, sobretudo, de como as informações foram obtidas e preservadas. O respeito aos direitos fundamentais na investigação digital não representa obstáculo à justiça penal, mas constitui condição essencial de sua própria legitimidade democrática, reafirmando que, no Estado Democrático de Direito, os fins não justificam os meios.

REFERÊNCIAS

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidência da República, 1988.

BRASIL. Lei nº 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. *Diário Oficial da União*, Brasília, DF, 25 jul. 1996.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. *Diário Oficial da União*, Brasília, DF, 24 abr. 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*, Brasília, DF, 15 ago. 2018.

BRASIL. Lei nº 13.964, de 24 de dezembro de 2019. Pacote Anticrime. *Diário Oficial da União*, Brasília, DF, 26 dez. 2019.

CAMARGO, Coriolano. *Direito Digital e Processo Eletrônico*. São Paulo: Editora RT, 2021.

CAPPELLETTI, Mauro; GARTH, Bryant. *Acesso à justiça*. Porto Alegre: Fabris, 1988.

COMPARATO, Fábio Konder. *A afirmação histórica dos direitos humanos*. 6. ed. São Paulo: Saraiva, 2005.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). *Justiça em Números 2023*. Brasília: CNJ, 2023. Disponível em: <https://www.cnj.jus.br>. Acesso em: 7 maio 2025.

LOPES JR., Aury. *Direito Processual Penal*. 20. ed. São Paulo: Saraiva, 2023.

MARINONI, Luiz Guilherme. *A efetividade do processo*. 4. ed. São Paulo: RT, 2014.

PECK, Patrícia. *Direito Digital*. 7. ed. São Paulo: Saraiva, 2021.

SANTOS, Boaventura de Sousa. *Sociologia jurídica crítica: para um novo senso comum em direito*. 4. ed. São Paulo: Cortez, 2007.

SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais*. 11. ed. Porto Alegre: Livraria do Advogado, 2012.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. *Curso de direito constitucional*. 11. ed. São Paulo: Saraiva, 2022.

BRASIL. Supremo Tribunal Federal (2. Turma). Habeas Corpus nº 168.052/SP. Rel. Min. Gilmar Mendes. Brasília, DF: STF, 2019.

BRASIL. Supremo Tribunal Federal (Plenário). Recurso Extraordinário nº 1.055.941/SP. Tema 987. Rel. Min. Gilmar Mendes. Brasília, DF: STF, 2019.

BRASIL. Supremo Tribunal Federal (Plenário). Ação Direta de Inconstitucionalidade nº 5527. Rel. Min. Rosa Weber. Brasília, DF: STF, 2016.

BRASIL. Superior Tribunal de Justiça (6. Turma). Habeas Corpus nº 598.051/SP. Rel. Min. Ribeiro Dantas. Brasília, DF: STJ, 2020.

BRASIL. Superior Tribunal de Justiça (6. Turma). Recurso em Habeas Corpus nº 51.531/SP. Rel. Min. Rogerio Schietti Cruz. Brasília, DF: STJ, 2015.

BRASIL. Superior Tribunal de Justiça (6. Turma). Recurso em Habeas Corpus nº 133.430/PE. Brasília, DF: STJ, 2021.

BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 1.785.311/SP. Rel. Min. Nancy Andrighi. Brasília, DF: STJ, 2019.

TEIXEIRA, Tarcísio. *Direito Digital e Processo Eletrônico*. 7. ed. São Paulo: Saraiva, 2022.

WATANABE, Kazuo. Acesso à Justiça e efetividade do processo. *Revista da EMERJ*, v. 2, n. 7, 1999.