UNIVERSIDADE FEDERAL DA PARAÍBA – UFPB
CENTRO DE CIÊNCIAS JURÍDICAS – CCJ
COORDENAÇÃO DO CURSO DE DIREITO – CAMPUS JOÃO PESSOA
COORDENAÇÃO DE MONOGRAFIA

MARIA EDUARDA MANGUEIRA CAMPOS

A ADMISSIBILIDADE DAS PROVAS DIGITAIS NO PROCESSO PENAL: LIMITES CONSTITUCIONAIS À LUZ DO *FISHING EXPEDITION* E DA SERENDIPIDADE

JOÃO PESSOA
2025

MARIA EDUARDA MANGUEIRA CAMPOS

A ADMISSIBILIDADE DAS PROVAS DIGITAIS NO PROCESSO PENAL: LIMITES CONSTITUCIONAIS À LUZ DO *FISHING EXPEDITION* E DA SERENDIPIDADE

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito de João Pessoa do Centro de Ciências Jurídicas da Universidade Federal da Paraíba como requisito parcial da obtenção do grau de Bacharel em Direito.

Orientadora: Dr.ª Lenilma Cristina Sena de Figueiredo Meirelles

JOÃO PESSOA
2025

Catalogação na publicação
Seção de Catalogação e Classificação

C198a Campos, Maria Eduarda Mangueira.
A admissibilidade das provas digitais no processo penal: limites constitucionais à luz do fishing expedition e da serendipidade / Maria Eduarda Mangueira Campos. - João Pessoa, 2025.
82 f.

Orientação: Drª Lenilma Cristina Sena de Figueiredo Meirelles.
TCC (Graduação) - UFPB/CCJ.

1. Prova digital. 2. Processo penal. 3. Cadeia de custódia. 4. Fishing expedition. 5. Serendipidade. I. Meirelles, Drª Lenilma Cristina Sena de Figueiredo. II. Título.

UFPB/CCJ CDU 34

Elaborado por Lucimário Dias dos Santos - CRB-15/645

MARIA EDUARDA MANGUEIRA CAMPOS

A ADMISSIBILIDADE DAS PROVAS DIGITAIS NO PROCESSO PENAL: LIMITES CONSTITUCIONAIS À LUZ DO *FISHING EXPEDITION* E DA SERENDIPIDADE

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito de João Pessoa do Centro de Ciências Jurídicas da Universidade Federal da Paraíba como requisito parcial da obtenção do grau de Bacharel em Direito.

Orientadora: Dr.ª Lenilma Cristina Sena de Figueiredo Meirelles

DATA DA APROVAÇÃO: 26 DE SETEMBRO DE 2025

BANCA EXAMINADORA:

Prof.ª Dr.ª LENILMA CRISTINA SENA DE FIGUEIREDO MEIRELLES
(ORIENTADORA)

Prof. Me. EDUARDO DE ARAÚJO CAVALCANTI
(AVALIADOR)

Prof. Dr. ROMULO RHEMO PALITOT BRAGA
(AVALIADOR)

Aos meus pais, Antenor e Shirley, dedico este trabalho, assim como dedicarei todos os feitos que ainda hão de se concretizar em minha vida. Dedico-o como quem oferece um fruto àqueles que semearam, cuidaram e regaram a árvore da minha existência. A conquista que hoje se realiza é reflexo da força silenciosa de seus sacrifícios e da grandeza do amor que me sustenta. Tudo o que sou,e tudo o que ainda serei, traz em si a marca eterna da vossa dedicação.

AGRADECIMENTOS

Agradeço primeiramente a Deus, que em sua infinita bondade me permitiu ingressar na faculdade e no curso dos meus sonhos, sustentando-me até a conclusão desta etapa tão importante. A Ele, pelo amor incondicional e ilimitado, mesmo diante das minhas falhas.

Agradeço também à minha Mãe, Maria Santíssima, que me escuta, me entende e me acolhe em seu regaço amoroso, intercedendo por todas as minhas necessidades e desejos mais íntimos.

Sou imensamente grato aos meus pais, Antenor e Shirley, pela doação de uma vida inteira. Por cada dia de trabalho, por cada gota de suor e por todas as batalhas travadas para que a educação fosse o caminho do crescimento. Por todo amor, cuidado e incentivo, os quais passarei a vida tentando retribuir, ainda que nunca consiga alcançar a grandeza do que recebi.

Aos meus irmãos, Samuel e Antenor Neto, que, cada um à sua maneira, me ensinam e me inspiram a ser melhor a cada dia.

Ao meu avô, Antenor Campos, in memoriam, agradeço por ter me mostrado a beleza da simplicidade, do esforço e do trabalho honrado. Sei que, do céu, se orgulha desta conquista como sempre se orgulhou de mim em vida.À minha avó Rosinha, pelo exemplo de força e pela alegria sincera com que sempre me recebeu, fazendo de cada visita um momento de acolhimento e afeto.

Ao meu avô Décio, agradeço por ter caminhado tão de perto comigo ao longo da vida, por transformar a simplicidade em felicidade e por me lembrar, em cada gesto, do quanto acredita que eu irei longe.À minha avó Maria do Socorro, sou grata pelos incontáveis momentos compartilhados, pela ternura que consola, pelo cuidado constante e pelo amor sem medidas. Obrigada por se alegrar com minhas conquistas e por dividir comigo o peso das minhas dores.

Aos meus tios e familiares, deixo minha gratidão, em especial ao meu padrinho Júlio Serpa, com quem compartilho a caminhada jurídica. É ele quem, com palavras sábias e incentivo constante, me orienta e me encoraja a ir além. À minha

tia Samara, igualmente colega do Direito, agradeço pela presença firme e pela torcida generosa pelo meu sucesso.

Agradeço ao meu melhor amigo, namorado e colega de turma, André Maracajá, pelo apoio diário, pelos constantes incentivos, pela parceria fiel nos estudos e na vida, por estar ao meu lado em todos os momentos e por se alegrar com minhas conquistas como se fossem suas. Não poderia ter escolhido um companheiro melhor para trilhar comigo este caminho.

Ao grupo Filhas de São Carlo Acutis, na pessoa da minha formadora Ellcana Almeida, pela intercessão constante e por guiarem e fortalecerem meu caminho de fé, impulsionando-me a crescer espiritualmente a cada passo.

Às minhas amigas Ana Clara Nóbrega, Maria Gabriela Nasiasene, Júlia Melo, Maria Laura Carvalho, Juliana Belota e Luma Nunes, agradeço por sonharem este sonho comigo, por compreenderem minhas ausências e por estarem sempre na primeira fila para me aplaudir. A amizade de vocês é um presente de Deus em minha vida.

Aos amigos que o curso me deu, especialmente o “Grupo Top”, nas pessoas de André Maracajá, Daniel Prado, Laura Beatriz, Lucas Toscano e Luciano Henrique,agradeço por tornarem a caminhada mais leve e os dias difíceis mais suportáveis. É uma verdadeira honra concluir esta etapa ao lado de vocês.

À minha orientadora, professora Lenilma Meireles, por me apresentar o processo penal de forma tão brilhante e por aceitar caminhar comigo neste trabalho.

E, por fim, ao Gabinete da 9ª Vara Cível da Capital, nas pessoas de Dra. Adriana Lóssio, Elisa Cristina, Laura Carolina, Lucianne Solano e Germana Lins, pela acolhida generosa e pela oportunidade diária de aprendizado e crescimento.

“Sonhai e ficareis aquém”

São José Maria Escrivá

RESUMO

O presente Trabalho de Conclusão de Curso tem por objetivo examinar a admissibilidade das provas digitais no processo penal, com foco nos limites constitucionais impostos à sua obtenção e utilização, especialmente à luz das práticas da fishing expedition e do princípio da serendipidade. O primeiro capítulo dedica-se à análise da prova digital e de seus limites constitucionais, apresentando seu conceito, características e natureza jurídica, as principais formas de obtenção, os cuidados relativos à cadeia de custódia e, ainda, os direitos e garantias fundamentais que funcionam como limites à atuação estatal. O segundo volta-se ao estudo da fishing expedition, explorando sua origem, hipóteses de ocorrência no ambiente digital e os reflexos da prática na colisão com os direitos fundamentais. O terceiro capítulo aborda a serendipidade digital, expondo sua origem e conceito, as posições doutrinárias sobre a aceitação da prova fortuita, os critérios de validade de sua utilização no processo penal, bem como sua distinção em relação à fishing expedition, com especial atenção aos riscos trazidos pelos mandados judiciais genéricos. A pesquisa vale-se do método dedutivo, com predominância da pesquisa bibliográfica e documental, recorrendo a doutrina especializada, julgados e instrumentos normativos nacionais e internacionais. Conclui-se que, embora as provas digitais sejam cada vez mais relevantes para a persecução penal contemporânea, a sua admissibilidade deve estar condicionada a parâmetros constitucionais rígidos, de modo a assegurar a legitimidade da jurisdição penal, a proteção dos direitos fundamentais e o equilíbrio entre eficiência investigativa e garantias individuais.

Palavras-chave:prova digital; processo penal; cadeia de custódia; *fishing expedition;* serendipidade.

ABSTRACT

This Final Course Project aims to examine the admissibility of digital evidence in criminal proceedings, focusing on the constitutional limits imposed on its collection and use, especially in light of the practices of fishing expedition and the principle of serendipity. The first chapter is devoted to the analysis of digital evidence and its constitutional boundaries, presenting its concept, characteristics, and legal nature, the main forms of collection, the safeguards related to the chain of custody, and the fundamental rights that serve as limits to state action. The second one addresses fishing expedition, exploring its origin, possible occurrences in the digital environment, and the effects of such practice when colliding with fundamental rights. The third chapter discusses digital serendipity, presenting its origin and concept, the doctrinal positions regarding the acceptance of fortuitous evidence, the criteria for its admissibility in criminal proceedings, as well as its distinction from fishing expedition, with special attention to the risks posed by generic court orders. The research adopts the deductive method, with a predominantly bibliographic and documentary approach, relying on specialized legal scholarship, case law, and national and international normative instruments. It concludes that although digital evidence has become increasingly relevant in contemporary criminal prosecution, its admissibility must be subject to strict constitutional parameters, so as to ensure the legitimacy of criminal jurisdiction, the protection of fundamental rights, and the balance between investigative efficiency and individual guarantees.

Key-words:digital evidence; criminal procedure; chain of custody; fishing expedition; serendipity.

SUMÁRIO

1 INTRODUÇÃO

O avanço tecnológico das últimas décadas trouxe profundas transformações às relações sociais, econômicas e jurídicas, consolidando o ambiente digital como espaço central da vida contemporânea. A crescente utilização de meios eletrônicos para comunicação, armazenamento de dados e realização de transações modificou não apenas a dinâmica da vida cotidiana, mas também os mecanismos de persecução penal. Nesse novo cenário, tornou-se inevitável o enfrentamento da temática das provas digitais, em especial no que concerne à sua admissibilidade no processo penal e aos limites constitucionais que devem ser observados para que tais elementos de informação sejam considerados legítimos.

A ausência de regulamentação legal específica no Brasil para lidar com as peculiaridades das provas digitais acentua a complexidade do tema. Embora existam normas como a Lei nº 9.296/1996, que disciplina a interceptação telefônica, a previsão do Código de Processo Penal acerca das buscas e apreensões e as disposições do Marco Civil da Internet (Lei nº 12.965/2014), tais instrumentos não são suficientes para abarcar todas as particularidades que envolvem a coleta, a custódia e a utilização de provas oriundas do ambiente eletrônico. Essa lacuna normativa abre espaço para discussões acerca da compatibilidade das diligências investigativas com os direitos e garantias fundamentais, como a intimidade, a privacidade, a inviolabilidade das comunicações e a inadmissibilidade das provas ilícitas.

A problemática que emerge, portanto, consiste em definir quais critérios devem orientar a admissibilidade das provas digitais no processo penal, de modo a evitar que práticas abusivas, como o chamado *fishing expedition*, sejam mascaradas sob a aparência de legalidade, ao mesmo tempo em que se permite o aproveitamento legítimo de elementos fortuitamente encontrados em diligências regulares, fenômeno identificado como serendipidade.

Nesse ponto, a dificuldade prática está em estabelecer parâmetros que diferenciem,de maneira objetiva, a prova fortuita admissível da prova ilícita obtida por desvio de finalidade, sobretudo quando se trata do exame de dispositivos

eletrônicos ou de dados armazenados em nuvem, cuja vastidão e interdependência tornam tênue a linha divisória entre a legalidade e a violação de direitos.

Diante desse cenário, a presente pesquisa tem como objetivo analisar a admissibilidade das provas digitais no processo penal à luz da Constituição Federal, considerando os limites impostos pelos direitos e garantias fundamentais, em especial a intimidade, a privacidade, o sigilo das comunicações e a vedação a provas ilícitas. Busca-se, ainda, examinar a admissibilidade da prova digital diante dos fenômenos da serendipidade e do *fishing expedition,* a fim de delimitar em que circunstâncias tais elementos podem ser admitidos ou afastados do processo penal.

Para alcançar tais finalidades, a metodologia adotada combina pesquisa bibliográfica e documental, de natureza qualitativa, descritiva e crítica. A investigação parte do método dedutivo, com base na análise de legislações nacionais, em julgados paradigmáticos dos Tribunais Superiores e em documentos normativos, de modo a oferecer um panorama que permita compreender os desafios do tema. O estudo utiliza, ainda, revisão bibliográfica selecionada de obras doutrinárias e artigos acadêmicos voltados à temática da prova digital, ao mesmo tempo em que examina decisões recentes relacionadas à serendipidade e ao combate ao *fishing expedition*.

O trabalho foi estruturado em três capítulos centrais. No primeiro, examina-se o conceito, as características e a natureza jurídica da prova digital, bem como as principais formas de sua obtenção, a cadeia de custódia e os direitos e garantias fundamentais que funcionam como limites à atuação estatal. O segundo capítulo, por sua vez, é dedicado ao estudo do *fishing expedition*, desde sua origem e conceito até as hipóteses de ocorrência no ambiente digital e os reflexos sobre a validade das provas produzidas.

Por fim, o terceiro capítulo dedica-se ao exame da serendipidade digital e da admissibilidade da prova fortuita, explorando sua origem e conceituação, as diferentes posições doutrinárias e os entendimentos firmados na jurisprudência, bem como os critérios que condicionam sua validade. Também são analisadas a distinção em relação à prática do *fishing expedition* e as implicações decorrentes da

expedição de mandados judiciais genéricos, cujo caráter impreciso representa risco significativo à legalidade da investigação e à preservação dos direitos fundamentais.

A partir dessa organização, pretende-se oferecer uma visão abrangente e crítica sobre a admissibilidade das provas digitais no processo penal brasileiro, contribuindo para o debate acadêmico e para a reflexão prática acerca de um tema que se mostra cada vez mais atual e desafiador no contexto de uma sociedade marcada pela centralidade da informação e pelo avanço contínuo das tecnologias digitais.

2 A PROVA DIGITAL E OS LIMITES CONSTITUCIONAIS À SUA OBTENÇÃO

O Direito, enquanto reflexo das transformações sociais, políticas e econômicas de uma determinada época, vem sendo profundamente impactado pela consolidação da era digital.Embora no passado o poder estivesse concentrado nas autoridades religiosas ou no capital industrial,na contemporaneidade,ele se estrutura a partir do controle informacional, o qual está intrinsecamente ligado ao progresso tecnológico (Pinheiro,2021).

Desde o advento da internet, na segunda metade do século XX, as possibilidades de comunicação e armazenamento de dados cresceram consideravelmente, em virtude da conectividade e instantaneidade promovidas pelas redes sociais (Minto,2021). Em decorrência disso, dispositivos eletrônicos como computadores, smartphones e servidores em nuvem passaram a armazenar e concentrar informações de múltiplas naturezas, tais como comunicações privadas, transações financeiras, dados de geolocalização e arquivos pessoais, capazes de revelar inúmeros aspectos da vida íntima dos indivíduos.

Essas inovações resultantes da era digital impuseram significativas mudanças nos métodos de persecução penal, especialmente no que tange à produção e à admissibilidade da prova digital, que assumiu posição de destaque nas investigações contemporâneas. No entanto, a crescente importância dessa espécie probatória exige que a sua obtenção e utilização se submetam aos limites constitucionais delineadores dos direitos e liberdades individuais.Isso decorre do fato de que a possibilidade de monitoramento de comunicações privadas, a localização em tempo real de dispositivos e o acesso a dados sensíveis possuem grande potencial lesivo à intimidade e privacidade, exigindo, portanto, um controle jurídico rigoroso e a compatibilização com os princípios do devido processo legal, especialmente frente à lacuna normativa existente e às controvérsias ainda presentes na jurisprudência nacional.

Nesse contexto, o presente capítulo objetiva delimitar o conceito, as principais características e natureza jurídica das provas digitais, com vistas a uma melhor compreensão do instituto e de suas implicações processuais. Na sequência,

serão abordadas duas das formas de obtenção da prova digital**,**a busca e apreensão de dispositivos eletrônicos e o acesso remoto por meio de malwares ou o chamado “hacking estatal”**.**Ademais, será ressaltada a relevância da preservação da cadeia de custódia das evidências digitais, considerando que a sua fragilidade e volatilidade exigem atenção especial para garantir sua autenticidade e confiabilidade enquanto meio probatório.

Por fim, o capítulo tratará dos limites constitucionais que devem nortear a atuação estatal na obtenção de provas digitais, destacando a proteção da intimidade, do sigilo das comunicações e do direito à não autoincriminação, além de discutir a inadmissibilidade de provas obtidas por meios ilícitos, tendo em vista que as referidas garantias fundamentais não podem ser vistas como entraves à atuação investigativa, mas como marcos que asseguram a legitimidade do processo penal em um Estado Democrático de Direito.

2.1 CONCEITO, CARACTERÍSTICAS E NATUREZA JURÍDICA DA PROVA DIGITAL

A Constituição Federal de 1988 consagrou um modelo processual penal que se estrutura a partir de garantias fundamentais voltadas à proteção do acusado e à limitação do poder punitivo estatal. Princípios como a ampla defesa, contraditório, presunção de inocência e a separação entre as funções de acusar e julgar,previstos, especialmente, nos incisos LIII, LIV, LV e LVII do artigo 5º da Carta Magna, revelam a adoção de um sistema tipicamente acusatório. (Brasil,1988)

Tal orientação normativa foi reforçada pela edição da Lei nº 13.964/2019 (Pacote Anticrime), que acrescentou ao Código de Processo Penal o artigo 3º-A, cuja redação estabelece expressamente que: “Art. 3º-A. O processo penal terá estrutura acusatória, vedadas a iniciativa do juiz na fase de investigação e a substituição da atuação probatória do órgão de acusação.”

A despeito dessa afirmação legal, o Supremo Tribunal Federal, no julgamento das ADIs 6.298, 6.299, 6.300 e 6.305, realizado em 24/08/2023, conferiu interpretação conforme ao artigo 3º-A do CPP, permitindo que o juiz, de forma

pontual e nos limites legalmente autorizados, determine diligências suplementares para esclarecer dúvida relevante à formação do juízo de mérito.

Tal entendimento, contudo, tem sido alvo de duras críticas doutrinárias. Aury Lopes Jr. (2025) considera que essa posição do STF representa uma contradição estrutural, pois enfraquece a principal característica do sistema acusatório, qual seja, a separação entre as funções de acusar e julgar,ao permitir que o juiz atue na produção de provas, conduta típica do modelo inquisitório.

No entanto,ainda que persistam divergências interpretativas sobre o alcance da atuação judicial na fase instrutória, prevalece o entendimento de que o sistema acusatório é o paradigma normativo adotado pelo ordenamento jurídico brasileiro. Nesse modelo, incumbe às partes a condução da atividade probatória, ao passo que o magistrado deve manter postura imparcial, decidindo com base nos elementos válidos produzidos pelas partes.

Nesse contexto, a prova assume papel central no processo penal, constituindo o principal instrumento para a reconstrução dos fatos e formação do convencimento judicial. Etimologicamente, o termo *prova* deriva do latim *probatio*, que remete à ideia de verificação ou demonstração da veracidade de determinada alegação.

No âmbito jurídico, essa concepção traduz-se como o conjunto de atos processuais destinados a demonstrar a ocorrência ou a inexistência de fatos juridicamente relevantes. A esse respeito, Capez (2024) define a prova como o conjunto de atos praticados pelas partes, pelo juiz (nos limites legais) e por terceiros, como os peritos, voltados a formar a convicção do magistrado acerca da veracidade ou falsidade de um fato ou afirmação trazida ao processo.

Nessa mesma perspectiva, a prova é compreendida como instrumento voltado à reconstrução de um fato pretérito. Trata-se de uma função retrospectiva, na qual os elementos de convicção são utilizados para formar um juízo sobre acontecimentos passados. Lopes Jr. (2025) observa que o processo penal atua como um mecanismo de reconstituição aproximada de fatos históricos, servindo como ritual que visa instruir o julgador por meio da análise de elementos probatórios. Desse modo, a atividade probatória cumpre papel essencial na efetivação do

processo penal democrático, configurando-se como meio legítimo para a verificação dos fatos submetidos à apreciação judicial.

Tendo em vista a centralidade que as provas exercem na persecução penal e o seu protagonismo na formação do convencimento judicial, é inegável que a incorporação das tecnologias da informação ao cotidiano das relações humanas impactou diretamente na configuração dos meios probatórios. A massificação das interações digitais, a virtualização das atividades sociais e a digitalização de registros transformaram a forma como os fatos são documentados e investigados. Como consequência, a utilização das chamadas provas digitais passou a ser cada vez mais frequente no processo penal brasileiro. Todavia, a ausência de regulamentação específica sobre seu conceito, admissibilidade e formas de produção tem gerado controvérsias relevantes e dificultado a consolidação de uma prática processual segura e uniforme.

Nesse cenário, as provas digitais revelam-se instrumentos indispensáveis para a apuração de delitos cometidos em ambientes virtuais ou que, de alguma forma, deixam rastros no meio digital. Sua ausência de tipicidade legal, entretanto, classifica-as como provas atípicas, nos termos da doutrina especializada. Assim, embora não previstas expressamente no Código de Processo Penal, são admitidas com base na regra do art. 369 do Código de Processo Civil, aplicada subsidiariamente, que autoriza a utilização de todos os meios legais e moralmente legítimos para a demonstração da verdade dos fatos.

Sob uma perspectiva conceitual, a prova digital pode ser compreendida como toda informação armazenada em dispositivos informáticos, que se encontre sob a posse do investigado ou de terceiros e que contenha dados úteis à elucidação dos fatos, abrangendo elementos relevantes à busca da verdade no processo penal (Furlaneto; Santos, 2020).

Essa concepção não se limita aos vestígios diretamente ligados a crimes cibernéticos, alcançando também infrações tradicionais que deixam registros no ambiente digital, como comunicações via aplicativos, dados de geolocalização, arquivos multimídia e transações eletrônicas, incluindo, ainda, informações

provenientes de dispositivos integrados à chamada “internet das coisas”[1], o que evidencia a amplitude do espectro digital no contexto probatório contemporâneo.

Em linha convergente, entende-se que a prova digital consiste em instrumento jurídico voltado a demonstrar a existência de um fato e suas circunstâncias, quando essas se manifestam, no todo ou em parte, por meio digital (Thamay; Tamer, 2022).

Para além da conceituação, as provas digitais apresentam atributos técnicos que as distinguem das provas tradicionais, impondo cuidados rigorosos em sua coleta, preservação e análise. Denise Vaz (2012) identifica como características essenciais: a imaterialidade, que decorre da ausência de suporte físico, por se tratar de dados representados em linguagem binária; a volatilidade, consubstanciada na suscetibilidade de alteração, supressão ou corrupção das informações, de forma intencional ou acidental; a possibilidade de clonagem, que permite a reprodução ilimitada dos dados, sem distinção entre original e cópia; e a necessidade de intermediação técnica, uma vez que a compreensão do conteúdo digital exige dispositivos e programas específicos para sua decodificação.

Tais peculiaridades não apenas evidenciam desafios de ordem técnica, mas também implicações jurídicas, sobretudo quanto à necessidade de assegurar a cadeia de custódia, requisito indispensável para a preservação da autenticidade e integridade da prova e que,dada a sua importância, será objeto de tópico próprio

Quanto à sua natureza jurídica, embora a prova digital seja frequentemente associada à prova documental, essa equiparação não se apresenta de forma absoluta, diante das particularidades técnicas e funcionais que lhe conferem identidade própria. Como observa Vaz (2012), tal enquadramento se mostra insuficiente, pois ignora aspectos essenciais das evidências digitais, que não se confundem com documentos tradicionais, demandando tratamento normativo e interpretativo adequado às suas singularidades.

Sendo assim, em razão da ausência de disciplina normativa específica, sua admissão no processo penal ocorre, em regra, pela aplicação analógica das

[1] A expressão *Internet das Coisas* (IoT, do inglês *Internet of Things*) designa a conexão de objetos físicos do cotidiano,como eletrodomésticos, veículos e maquinário industrial, a redes digitais, por meio de sensores, softwares e tecnologias de comunicação. Essa integração possibilita o envio e o recebimento de dados em tempo real, favorecendo a automação, o monitoramento remoto e a otimização de processos em diferentes contextos sociais e econômicos.

disposições previstas para os documentos, notadamente o art. 232 do CPP e o art. 422 do CPC, cujo §3º estende esse regime às mensagens eletrônicas impressas.

Diante dessas considerações, conclui-se que a prova digital, por sua relevância crescente e peculiaridades técnicas, exige um tratamento que conjugue rigor metodológico e observância às garantias constitucionais, assegurando equilíbrio entre a efetividade da persecução penal e a tutela dos direitos fundamentais. Esse entendimento encerra a análise do conceito, das características e da natureza jurídica das provas digitais, servindo de base para o tópico subsequente, voltado ao exame das formas de obtenção e aos desafios relacionados à sua produção em conformidade com a ordem jurídica.

2.2 FORMAS DE OBTENÇÃO DA PROVA DIGITAL

Considerando a crescente relevância das tecnologias digitais e sua inserção nas relações sociais contemporâneas, multiplica-se, de forma significativa, a variedade de meios pelos quais se torna possível a obtenção das chamadas provas digitais, já conceituadas no capítulo precedente. A análise dessas modalidades reveste-se de importância central para o presente estudo, uma vez que a forma de produção e coleta da prova influencia diretamente sua validade jurídica. Com efeito, a compatibilidade entre o método empregado e os direitos constitucionalmente assegurados constitui requisito indispensável para a admissibilidade do elemento probatório, cuja inobservância pode acarretar a sua nulidade.

Entre as formas atualmente reconhecidas e mais utilizadas na persecução penal, destacam-se a interceptação de comunicações telemáticas; a obtenção de dados mediante apreensão física do dispositivo eletrônico; a requisição de informações a terceiros, especialmente aos provedores de conexão e de aplicações de internet; e a instalação de programas espiões (*malwares)* em dispositivos eletrônicos , com a finalidade de coleta remota de dados.

Não obstante a relevância e a diversidade de cada uma dessas modalidades, o presente trabalho concentra sua análise em duas delas: a obtenção de provas digitais por meio da apreensão física do dispositivo eletrônico e a utilização de técnicas de acesso oculto a aparelhos informáticos. Tal recorte se

justifica não apenas pela atualidade dos temas, mas também pela complexidade jurídica e pelos desafios processuais que ambas ensejam, exigindo exame detido quanto aos limites de sua utilização e aos parâmetros necessários para compatibilizá-las com as garantias constitucionais e processuais penais.

2.2.1 Busca e apreensão de dispositivos informáticos

O acesso a dados armazenados em aplicativos de comunicação, como WhatsApp, Instagram, Telegram e Twitter, bem como a outras informações constantes em dispositivos eletrônicos, frequentemente decorre da apreensão física desses aparelhos, notadamente em decorrência da execução de mandados de busca e apreensão. Esse instituto, embora comumente tratado de forma unitária, comporta duas figuras distintas: a busca e a apreensão.

Enquanto a busca consiste no procedimento voltado à localização de pessoas ou objetos relevantes à investigação, a apreensão refere-se à retirada desses elementos da esfera de disponibilidade do investigado, para posterior análise e utilização probatória. Embora disciplinada pelo Código de Processo Penal, a regulamentação legal privilegia a figura da busca, prevendo, no art. 240, § 1º, alíneas “b”, “c”, “d”, “f” e “g”, as hipóteses em que se autoriza a apreensão, sem, contudo, esgotar suas finalidades. É possível, inclusive, que ambas ocorram separadamente, como na busca destinada à captura de pessoa ou na apreensão resultante de entrega voluntária do objeto (Smanio, 2022).

A busca, nesse sentido, configura meio de obtenção de prova destinado a localizar elementos que possam contribuir para a formação da convicção judicial. Tradicionalmente, a legislação prevê duas modalidades principais: a domiciliar e a pessoal, sem excluir, contudo, outras formas, como a busca de dados e arquivos digitais. Em qualquer caso, a medida deve observar parâmetros rigorosos, como a reserva de jurisdição e a subsidiariedade dos meios de obtenção de prova, avaliando-se, no caso concreto, os limites da restrição aos direitos fundamentais e a proporcionalidade da intervenção, de modo a compatibilizar a eficácia investigativa com as garantias constitucionais (Smanio, 2022).

Nesse cenário, considerando que dispositivos eletrônicos como smartphones, tablets e computadores se tornaram, no cotidiano contemporâneo,

extensões quase indissociáveis da esfera privada do indivíduo, emergem relevantes questionamentos jurídicos quanto aos limites impostos à atuação estatal. Discute-se se a apreensão física do equipamento, por força de mandado judicial, autoriza, de forma automática, o acesso aos dados nele contidos, bem como se o encontro fortuito do aparelho em local relacionado ao fato delituoso legitima o acesso investigativo por parte das autoridades, e, ainda, em que medida o consentimento livre e expresso do titular dos dados pode suprir a necessidade de autorização judicial para a realização da diligência.

No que concerne à possibilidade de acesso ao conteúdo armazenado em dispositivos eletrônicos apreendidos, o Supremo Tribunal Federal, em um primeiro momento, adotou entendimento de que seria legítima a extração de registros telefônicos gravados em aparelho celular obtido durante prisão em flagrante, independentemente de ordem judicial, por entender que não se tratava de comunicação protegida pelo sigilo, mas sim de dados em si mesmos (STF,2012).

Contudo, a rápida evolução tecnológica e a centralidade do celular como repositório de múltiplas esferas da vida pessoal e profissional determinaram a necessidade de revisão desse entendimento. Em 2016, o Superior Tribunal de Justiça consolidou orientação em sentido oposto, reconhecendo como ilícita a devassa de dados, inclusive conversas de aplicativos, realizada diretamente pela polícia em celulares apreendidos sem prévia autorização judicial (STJ,2016), fundamentando-se nos direitos à inviolabilidade da comunicação e à privacidade, previstos tanto no art. 5º, XII, da Constituição Federal quanto no Marco Civil da Internet (Lei nº 12.965/2014), especialmente em seu art. 7º, incisos II e III, in verbis:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
>
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

Assim, resta consolidada a orientação de que, ainda que o dispositivo eletrônico tenha sido regularmente apreendido, a análise de seu conteúdo, notadamente dos dados armazenados, requer ordem judicial específica e

fundamentada, não se admitindo buscas automáticas ou genéricas, ainda que em situações de flagrante delito,sob pena de incorrer na prática ilegal de fenômeno denominado como *“Fishing Expedition”*, que será objeto de capítulo próprio posteriormente. Tal entendimento se coaduna com a doutrina que destaca a imprescindibilidade da autorização judicial como requisito de legitimidade da diligência, diante da potencial restrição a direitos fundamentais do investigado (Jangutta, 2019).

Em relação à hipótese de acesso a aparelho celular deixado fortuitamente na cena do crime, destaca-se recente decisão do Supremo Tribunal Federal, proferida no julgamento do ARE 1.042.075/RJ (Tema 977 da repercussão geral), que firmou orientação de significativa repercussão para o processo penal brasileiro. O Tribunal assentou que, na ocorrência do encontro casual de dispositivo eletrônico em local relacionado ao fato delituoso, é legítimo o acesso, pela autoridade policial, aos registros e informações ali armazenados, independentemente de prévia autorização judicial, desde que tal diligência se restrinja à identificação da autoria do crime ou do proprietário do aparelho (STF,2025).

Acrescenta-se, no entanto, a ressalva quanto à necessidade de comunicação e justificação subsequente da medida ao Poder Judiciário, o que demonstra a busca por um ponto de equilíbrio entre a efetividade da investigação criminal e a proteção dos direitos fundamentais. Tal exigência revela a determinação do Tribunal de que a atuação investigativa seja pautada pelo rigor e pela proporcionalidade, restringindo o acesso ao conteúdo do aparelho às hipóteses em que tal providência seja estritamente indispensável à elucidação do crime. Ao mesmo tempo, o julgado reconhece a licitude da prova obtida de forma fortuita, legitimando o fenômeno da serendipidade e conferindo respaldo à atuação policial quando esta se mantenha nos limites constitucionais que tutelam a intimidade, a privacidade e a proteção dos dados pessoais.

Além disso, a autorização conferida à autoridade policial para a adoção de providências voltadas à preservação dos dados e metadados, bem como a determinação de apreciação prioritária dos pedidos dessa natureza pelo Judiciário, revelam a contemporaneidade do conteúdo da decisão, demonstrando sensibilidade à volatilidade dos dados digitais e à necessidade de celeridade na atuação estatal para evitar o perecimento da prova.

Por outro lado, no que se refere à controvérsia acerca da possibilidade de o consentimento do acusado suprir a necessidade de autorização judicial para o acesso a dados armazenados em aparelhos celulares apreendidos, a Suprema Corte consignou que, nos casos em que o dispositivo eletrônico é apreendido na posse do investigado,seja em virtude do art. 6º do Código de Processo Penal ou em decorrência de prisão em flagrante, o acesso ao conteúdo dos dados pode ser legitimamente efetuado sem ordem judicial, desde que haja consentimento expresso, livre e esclarecido do titular. Ressalta-se, entretanto, que tal manifestação de vontade deve ser inequívoca, não podendo ser presumida nem decorrer de eventual constrangimento ou da ausência de informação adequada quanto à extensão e aos limites da medida autorizada.

Diante de todo o exposto, evidencia-se que o acesso a dados armazenados em dispositivos eletrônicos apreendidos, seja em virtude de mandado judicial, de encontro fortuito na cena do crime ou de consentimento do titular, deve estar submetido a critérios estritos de legalidade, necessidade e proporcionalidade, de modo a garantir a harmonização entre a eficiência investigativa e a tutela dos direitos fundamentais, além de adequar-se aos constantes desafios impostos pela tecnologia.

Superada a análise das questões atinentes à apreensão do suporte físico, passa-se, no tópico seguinte, ao exame da obtenção da prova digital mediante acesso oculto, especialmente por meio de softwares espiões (malwares), modalidade que suscita peculiaridades técnicas e relevantes discussões jurídicas quanto aos limites da atuação estatal no ambiente digital.

2.2.2 Acesso remoto e oculto por *hacking* estatal e *malwares*

A ampliação do uso de tecnologias digitais na prática de ilícitos impôs aos órgãos de persecução penal o desafio de adotar métodos de investigação cada vez mais sofisticados. Para além das diligências convencionais, como a apreensão física de dispositivos eletrônicos, tornou-se viável a obtenção de provas mediante acesso oculto e remoto a dados sensíveis, possibilitando a superação de barreiras técnicas que tradicionalmente protegiam tais informações. Essas estratégias surgem como resposta ao fortalecimento da criminalidade organizada, à complexidade dos crimes

transnacionais e à crescente sofisticação dos mecanismos empregados para ocultar provas, exigindo do Estado a implementação de técnicas capazes de alcançar dados armazenados em sistemas cada vez mais complexos e protegidos por avançados recursos de segurança.

Nesse cenário, destacam-se duas práticas investigativas de particular relevância: o *hacking* estatal e a infiltração por *malwares.* Apesar de ambas visarem a obtenção remota e sigilosa de informações, esses instrumentos não se confundem, apresentando particularidades quanto ao modo de execução e aos riscos envolvidos.O *hacking,* enquanto técnica, consiste na exploração, por agentes estatais, de vulnerabilidades presentes em programas ou dispositivos conectados à internet, possibilitando o acesso remoto não autorizado enquanto perdurar a conexão ativa.

Em contraste, a infiltração por *malware* caracteriza-se pela instalação dissimulada de programa espião no sistema-alvo, o que cria um “portal” de acesso remoto,comumente denominado de *“backdoor”*, viabilizando o monitoramento contínuo e a coleta de informações mesmo na ausência de conexão constante à rede, o que pode ocorrer por diferentes meios, como o acoplamento de hardware ao dispositivo, a visita a sites vulneráveis ou o download de arquivos infectados.(Ramalho, 2017, *apud* Smanio, 2022).

Diante desse quadro, a principal distinção entre os métodos em análise reside no fato de que o *hacking* estatal pressupõe e está necessariamente vinculado à existência de conexão à internet, de modo que sua eficácia limita-se ao período em que o dispositivo-alvo permanece conectado à rede, enquanto os *softwares* espiões *(malwares),* uma vez instalados no sistema, são capazes de operar independentemente de conexão constante, permitindo a coleta e o monitoramento de informações a qualquer tempo, inclusive de modo automatizado e sem a necessidade de interação do usuário (Mendes, 2018).

Apesar dessas diferenças estruturais, ambos os mecanismos conferem às autoridades de persecução penal a possibilidade de monitoramento contínuo e remoto das funções do computador, inclusive quando o equipamento não se encontra em uso ativo. Isso abrange, por exemplo, o acionamento de microfones e *webcams*, a captação de sinais ambientais, o acompanhamento em tempo real de comunicações telemáticas e o acesso direto a arquivos, senhas e demais

informações armazenadas no dispositivo investigado (Smanio, 2022, *apud* Mendes, 2020).

Não há dúvidas, portanto, dos inúmeros benefícios advindos das referidas técnicas para o âmbito investigativo. Contudo, a utilização de métodos de obtenção de prova por meio de acesso oculto,suscita preocupações significativas quanto ao impacto sobre direitos fundamentais. Tratam-se de mecanismos dotados de elevada capacidade invasiva, aptos a acessar e coletar, de modo indiscriminado, vasto conjunto de dados pessoais, comunicações privadas e registros sensíveis dos investigados, frequentemente sem que estes sequer tenham ciência da medida, fator que enseja questionamentos quanto à legitimidade da relativização de garantias como a privacidade, o sigilo das comunicações e a proteção dos dados pessoais, pilares do Estado Democrático de Direito (Ribeiro;Cordeiro;Fumach, 2022).

No contexto brasileiro contemporâneo, para além do elevado grau de invasividade inerente às técnicas de acesso oculto, evidencia-se a ausência de regulamentação legal específica acerca desses métodos, circunstância que se revela verdadeiro óbice à sua adoção no âmbito da persecução penal.

A doutrina especializada é praticamente uníssona ao afastar a possibilidade de aplicação analógica das leis de interceptação telefônica e de organizações criminosas a tais procedimentos. A título exemplificativo, a Lei nº 9.296/1996, que disciplina as interceptações de comunicações, regula unicamente a captação prospectiva de ligações e mensagens, limitando-se ao monitoramento a partir do início da investigação e durante prazo judicialmente delimitado. Em contraste, o emprego de *malwares* possibilita acesso retrospectivo e irrestrito ao universo de dados armazenados nos dispositivos, extrapolando, assim, os contornos inicialmente concebidos para medidas probatórias invasivas (Abreu;Antonialli, 2017).

A Lei das Organizações Criminosas (Lei nº 12.850/2013), por sua vez, apesar de prever a infiltração de agentes em investigações voltadas à repressão de delitos praticados por organizações criminosas,condicionando sua aplicação à presença de indícios concretos, à demonstração da indispensabilidade do meio e à delimitação expressa do alcance operacional,não contempla, em nenhum de seus dispositivos, autorização específica para o *hacking* digital, a utilização de *malwares* ou o acesso oculto a sistemas informáticos. Assim, a ausência de referência normativa clara a essas técnicas pode conduzir à ilicitude das provas obtidas por tais meios, sobretudo diante da tipificação penal da invasão a dispositivo informático,

prevista no artigo 154-A do Código Penal, que não comporta qualquer exceção para fins de persecução criminal (Smanio, 2022).

Diante disso, verifica-se a necessidade de avanço na elaboração de marco normativo que discipline a utilização de tais métodos, a exemplo do que já ocorre em países como os Estados Unidos, Alemanha e Itália.Neste último, encontra-se em debate projeto de lei destinado a estabelecer critérios objetivos e salvaguardas para o uso do *hacking* estatal, prevendo, dentre outros pontos, a limitação da medida à investigação de crimes graves e por tempo determinado, a preservação do sigilo e integridade dos dados coletados, além de mecanismos diferenciados para as buscas digitais, reconhecendo a sua potencialidade de invasão superior às buscas físicas (Abreu;Antonialli, 2017).

Em suma, o contexto atual revela um cenário de insegurança jurídica quanto à licitude e à admissibilidade das provas obtidas por técnicas de acesso oculto no processo penal brasileiro, reforçando a premência de regulamentação específica. Tal medida é imprescindível não apenas para a proteção dos direitos dos investigados, mas também para a segurança jurídica da persecução penal, de modo a assegurar a idoneidade e a confiabilidade do trabalho investigativo.

Neste contexto, o próximo tópico abordará os aspectos centrais da cadeia de custódia da prova digital, ressaltando a importância de sua observância para a integridade e autenticidade dos elementos probatórios coletados, especialmente à luz das características específicas que permeiam os meios digitais.

2.3 A CADEIA DE CUSTÓDIA E A INTEGRIDADE DA PROVA DIGITAL

A cadeia de custódia, inserida no ordenamento jurídico brasileiro pelo Pacote Anticrime (Lei nº 13.964/2019), representa um avanço expressivo no âmbito das garantias processuais, ao assegurar a autenticidade e a integridade dos vestígios colhidos no curso da investigação criminal. Conforme preceitua o art. 158-A do Código de Processo Penal, considera-se cadeia de custódia “o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte” (Brasil, 2019).

A partir dessa definição, depreende-se que a cadeia de custódia traduz-se em um procedimento formal e sistemático de documentação das sucessivas etapas

por que passa a evidência criminal, justamente com o intuito de prevenir adulterações, extravios ou interferências que possam comprometer a confiabilidade e a licitude do elemento probatório (Lima, 2022). Ademais, a doutrina e a jurisprudência reconhecem que se trata do percurso indispensável a ser trilhado pela prova até sua apresentação ao magistrado competente, sendo certo que qualquer interferência indevida nesse trâmite processual pode ensejar a sua total imprestabilidade (STJ, 2019).

Nos dispositivos subsequentes ao art. 158-A do CPP, observa-se um detalhamento minucioso das fases que compõem a cadeia de custódia, abrangendo etapas como reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e, por fim, descarte dos vestígios. Tais procedimentos têm como finalidade precípua garantir a efetividade das garantias inerentes ao processo penal, destacando-se, dentre elas, a ampla defesa, o contraditório e, sobretudo, o direito à prova lícita.

Embora não se pretenda, neste trabalho, examinar exaustivamente cada uma dessas etapas, é imperioso reconhecer que o legislador, ao disciplinar a cadeia de custódia, restringiu seu campo de incidência, na medida em que a classificação de “vestígio” definida pelo §3º do art. 158-A do CPP como “todo objeto ou material bruto, visível ou latente, constatado ou recolhido, que se relaciona à infração penal” limita-se, em regra, às provas materiais, vinculando a exigência do procedimento, de modo mais direto, às provas de natureza pericial.

Todavia, embora os dispositivos legais tenham sido originalmente concebidos para a persecução de delitos convencionais, como roubo e homicídio, não se pode olvidar que a observância da cadeia de custódia também se impõe, por analogia, às provas digitais. Isso se torna ainda mais relevante diante da peculiar dinâmica das evidências digitais, as quais, em virtude de sua natureza volátil, imaterial e altamente suscetível à manipulação, exigem rigor redobrado no registro e na preservação de sua trajetória procedimental (Badaró, 2021).

Dessa forma, em face das peculiaridades inerentes às provas digitais, emergem desafios consideráveis que impõem a adoção de procedimentos diferenciados para assegurar sua idoneidade no processo penal. Conforme ressalta Badaró (2021), a ausência de materialidade e a “congênita mutabilidade” dos vestígios digitais exigem um rigor ainda maior quanto ao registro e à documentação

de todos os agentes e etapas envolvidos na manipulação da evidência, sob pena de comprometer irremediavelmente sua autenticidade e confiabilidade (Badaró, 2021).

Apesar do relevante avanço representado pela incorporação da cadeia de custódia ao Código de Processo Penal, o legislador brasileiro não instituiu, até o presente momento, procedimento específico para a custódia de provas digitais, restringindo-se a prever normas gerais aplicáveis a todo e qualquer tipo de vestígio. Essa lacuna normativa decorre, em grande medida, do dinamismo e da rápida evolução tecnológica, que dificultam a elaboração de regras fixas e detalhadas, sob pena de torná-las rapidamente obsoletas (Parodi, 2020, *apud* Smanio, 2021). Ainda assim, a doutrina processual penal é uníssona ao afirmar que a correta catalogação e preservação das provas digitais constitui requisito essencial, não apenas para afastar a ilicitude dos elementos probatórios, mas também para resguardar a confiança e a segurança do processo judicial.

Nesse contexto, merece destaque o Projeto de Lei nº 4.291/2020, que propõe alterações ao Código de Processo Penal para disciplinar de forma específica a custódia de elementos digitais de prova. A proposta estabelece protocolos tecnológicos voltados à preservação da integridade e autenticidade dos dados, veda fundamentações genéricas em pedidos e decisões judiciais e impõe requisitos claros para buscas, apreensões e acessos remotos, inclusive mediante técnicas como o hacking estatal.

Nessa mesma direção, ressalta-se a relevância da Norma ABNT NBR ISO/IEC 27037:2012, que, mesmo não possuindo força vinculante, consolida-se como referência técnica fundamental, reconhecida nacional e internacionalmente, para o tratamento das evidências digitais.

Tal disposição normativa preconiza princípios indispensáveis para a obtenção legítima da prova digital, notadamente: a auditabilidade, que se refere à possibilidade de averiguação da correta aplicação das técnicas forenses adotadas; a repetibilidade, consistente na capacidade de obtenção dos mesmos resultados, sob as mesmas condições e utilizando os mesmos procedimentos; a reprodutibilidade, que exige a produção dos mesmos resultados mesmo diante da utilização de instrumentos ou condições diversas; e a justificabilidade, que implica a necessidade de justificar tecnicamente os métodos e procedimentos empregados, assegurando a

adequação entre a metodologia escolhida e os resultados obtidos (Furlaneto e Santos, 2020).

Assim,os referidos parâmetros metodológicos, ao proporcionar transparência e segurança ao tratamento das evidências digitais, fortalecem a validade probatória das informações coletadas e servem de verdadeiro filtro para a admissibilidade das provas digitais no processo penal.

A jurisprudência pátria tem reiteradamente afirmado a necessidade de observância rigorosa da cadeia de custódia no tocante às provas digitais, reconhecendo que a sua inobservância acarreta a inadmissibilidade do material produzido. No AgRg no HC 828.054/RN (Rel. Min. Joel Ilan Paciornik, j. 23/04/2024), o Superior Tribunal de Justiça declarou ilícita a prova extraída de aparelho celular apreendido em investigação de tráfico de drogas, pois a autoridade policial limitou-se a efetuar capturas de tela (*prints*), sem adotar procedimentos técnicos adequados que assegurassem a integridade e a rastreabilidade dos dados. O acórdão destacou que a volatilidade das informações digitais impõe a utilização de métodos reconhecidos, como a extração forense acompanhada do cálculo de *hash*, sob pena de quebra da cadeia de custódia e consequente imprestabilidade da prova.

Na mesma linha, no RHC 143.169/RJ (Rel. Min. Messod Azulay Neto,Rel. p/ Acórdão Min. Ribeiro Dantas, j. 07/02/2023), a Corte concluiu serem inadmissíveis provas digitais obtidas sem qualquer registro documental dos procedimentos adotados pela polícia para a preservação de sua integridade, autenticidade e confiabilidade. O entendimento firmado foi o de que não se admite, no processo penal, a presunção de fidedignidade das evidências digitais quando inexistem elementos que demonstrem, de forma objetiva, o atendimento aos requisitos da cadeia de custódia.

Em outro precedente relevante, o AgRg no RHC 184.003/SP (Rel. Min. Daniela Teixeira, j. 10/12/2024), segundo Cavalcante (2025), o STJ reconheceu que a corrupção de parte dos arquivos digitais compromete a integralidade do material e inviabiliza sua utilização em juízo, reforçando que a falta de rastreabilidade e de comprovação de autenticidade retira da prova qualquer valor probatório.Essa orientação jurisprudencial demonstra que a inobservância da cadeia de custódia não

constitui mera irregularidade formal, mas vício capaz de atingir a essência do elemento probatório, conduzindo, em regra, à sua exclusão do processo. Nesse ponto, a doutrina apresenta posicionamentos divergentes quanto às consequências dessa violação.

Para Badaró (2021), a ruptura desse encadeamento procedimental deve ser avaliada caso a caso, ponderando-se o grau de comprometimento da prova. Em hipóteses de irregularidades leves, a falha pode ser considerada apenas na valoração probatória, sem necessariamente ensejar a sua inadmissibilidade. Contudo, quando a ausência de documentação integral da cadeia de custódia gera dúvida objetiva acerca da autenticidade e da integridade da prova digital, impõe-se o seu desentranhamento, por ausência de idoneidade epistêmica. Em sentido diverso, Prado (2021) sustenta que, uma vez violada a cadeia de custódia, compromete-se a própria essência do elemento probatório, tornando-o inadmissível e insuscetível de apreciação judicial, nos termos do art. 157 do Código de Processo Penal.

Sob essa perspectiva, evidencia-se que a cadeia de custódia não é mero formalismo, mas um verdadeiro instrumento de proteção dos direitos fundamentais e de preservação da confiabilidade do processo penal. No próximo tópico, examinar-se-á de que forma tais exigências dialogam com as garantias constitucionais, notadamente a privacidade, a intimidade e o sigilo das comunicações, estabelecendo parâmetros objetivos para a atuação estatal no ambiente digital.

2.4 DIREITOS E GARANTIAS FUNDAMENTAIS COMO LIMITES À ATUAÇÃO ESTATAL

A constante evolução tecnológica, especialmente no campo da informática e das comunicações, modificou de forma profunda o cenário da persecução penal. A possibilidade de armazenar, processar e transmitir um volume massivo de informações em dispositivos eletrônicos trouxe ganhos inegáveis para a investigação criminal, mas, em contrapartida, propiciou um campo fértil para a tensão entre o interesse estatal na descoberta da verdade e a preservação dos direitos e garantias fundamentais.

Essa necessidade de equilíbrio entre a eficiência investigativa e a preservação da esfera de direitos do acusado não é inédita no processo penal, estando presente em diferentes modalidades de prova, inclusive nas mais tradicionais, como a busca e apreensão domiciliar, na qual, apesar do respaldo legal, ocorre a flexibilização da inviolabilidade do domicílio. No cenário digital, contudo, essa ponderação torna-se ainda mais complexa, dada a profundidade e a invisibilidade com que a tecnologia pode penetrar na vida privada do indivíduo, o que impõe atenção redobrada à observância das garantias constitucionais dos investigados.

Ademais, a coleta e o tratamento de dados digitais permitem acessar informações que ultrapassam aquelas visíveis ou conscientemente fornecidas pelo usuário, abrangendo, por exemplo, mensagens privadas, registros de geolocalização em tempo real, histórico de navegação, padrões de consumo e perfis comportamentais. Nesse sentido, como destacam Santos e Furlaneto (2024), a amplitude e a precisão dessas informações exigem um regime jurídico mais rigoroso do que aquele tradicionalmente aplicado às provas físicas ou documentais, sob pena de ampliar de forma desproporcional o poder de intrusão estatal.

Nas diversas formas de obtenção de provas digitais, desde a interceptação de comunicações telemáticas até a busca e apreensão de aparelhos eletrônicos, passando pela utilização de *malwares*, que permitem o acesso oculto a dispositivos, constatam-se, como ressaltam Furlaneto e Santos (2024), medidas potencialmente capazes de alcançar dados que extrapolam o objeto da investigação, atingindo a totalidade das informações armazenadas no dispositivo.

Essa característica, se não for contida por critérios objetivos e por rigoroso controle judicial, pode ocasionar grave comprometimento de direitos como a intimidade, a privacidade, o sigilo das comunicações e a proteção de dados pessoais, preocupação que se estende a todo o espectro das técnicas de obtenção de prova digital.

Diante disso, torna-se evidente que a admissibilidade das provas digitais relaciona-se de forma direta com a observância dos direitos e garantias fundamentais assegurados pela Constituição. Impõe-se, portanto, harmonizar a

eficiência investigativa com a proteção desses direitos, evitando que falhas procedimentais, como a ausência de autorização judicial ou o descumprimento das etapas da cadeia de custódia, resultem na perda de elementos relevantes para o processo.

Essa equação exige critérios claros e proporcionais, sob pena de comprometer tanto a efetividade da persecução penal quanto a credibilidade do próprio sistema de justiça. Diante da relevância da matéria, nos subtópicos seguintes examinar-se-á, de forma individualizada, cada uma dessas garantias constitucionais, evidenciando o seu papel como limite normativo à atuação estatal no ambiente digital.

2.4.1 Inviolabilidade à intimidade e à vida privada

A noção moderna de privacidade, conforme aponta Brito (2023), remonta ao século XVI, surgindo do processo de delimitação de uma esfera privada, livre da ingerência estatal, necessária ao desenvolvimento da personalidade humana. Trata-se, portanto, de um conceito relacional, que envolve a interação entre a personalidade de um indivíduo, as personalidades de outros e o mundo exterior, garantindo a todos um espaço de autonomia e resguardo contra formas de controle social (Doneda, 2019, *apud* Oliveira, 2021).

Fundamentadas nessa concepção inicial, resultante da separação entre a vida pública e a esfera pessoal, erigiram-se as modernas garantias constitucionais voltadas à proteção da intimidade e da vida privada. Sob essa perspectiva, o texto constitucional brasileiro consagra, no art. 5º, X, 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” (Brasil, 1988).

Tais garantias se articulam de forma interdependente com outras cláusulas constitucionais protetivas, como a inviolabilidade domiciliar (art. 5º, XI) e a inviolabilidade do sigilo das comunicações (art. 5º, XII). No presente subtópico, a análise concentrar-se-á na intimidade e na vida privada, enquanto o sigilo das comunicações será examinado no ponto subsequente, dada sua especificidade e a necessidade de abordagem individualizada. Já a inviolabilidade domiciliar, embora

relevante, apresenta reduzida pertinência no contexto digital, razão pela qual não será objeto de exame aprofundado neste trabalho.

Nessa linha, compreende-se a privacidade como “todas as manifestações da esfera íntima, privada e da personalidade”, consistindo no conjunto de informações que o indivíduo mantém sob seu controle e decide se, quando e como comunicará a terceiros (Silva, 1996, p. 202). Ainda que a Constituição de 1988 tenha conferido destaque à proteção da intimidade e da privacidade, é incontroverso que a evolução tecnológica e a inserção do “digital” no cotidiano humano impuseram novas dimensões e desafios a esses direitos. Tais desafios tornam-se particularmente evidentes no estabelecimento de critérios para a admissibilidade e a obtenção de provas digitais no processo penal, diante da tênue fronteira entre uma investigação eficiente e uma busca genérica e indiscriminada por elementos probatórios.

Como pontua Saad (2024), a privacidade, tradicionalmente concebida como liberdade negativa,exigindo apenas a abstenção de ingerências externas, demanda, atualmente, uma formulação positiva, impondo ao Estado o dever de atuar para assegurar sua efetiva proteção. Isso se deve ao fato de que os dados digitais, em virtude de seu amplo espectro e detalhamento, podem atingir de forma ainda mais incisiva a intimidade e a privacidade dos indivíduos (Vaz, 2012). Nesse cenário, é imprescindível que a atividade estatal, administrativa e jurisdicional, esteja estritamente conformada aos ditames constitucionais (PRADO, 2006), de modo a garantir o avanço da investigação criminal no ambiente digital ocorra de maneira equilibrada, preservando o núcleo essencial desses direitos e evitando que a eficácia da persecução penal se converta em pretexto para violações indevidas.

Diante desse panorama, impõe-se delimitar a abrangência do direito à intimidade e à vida privada, que, na atualidade, engloba todas as informações reveladoras de aspectos pessoais e reservados do indivíduo, estejam elas em comunicação ativa ou armazenadas de forma estática.

A doutrina, entretanto, tem estabelecido distinção entre os dados em trânsito,protegidos pelo sigilo das comunicações,e os dados estáticos, armazenados em dispositivos eletrônicos, cuja tutela se insere no âmbito do art. 5º, X, da Constituição Federal, relacionado à privacidade e à intimidade. Nesse sentido, o

Supremo Tribunal Federal consolidou entendimento no sentido de que dados não comunicados, mas armazenados, estão sob a égide da proteção à vida privada, sendo suficiente, para seu acesso, a prévia autorização judicial, não se exigindo lei específica, como ocorre nas hipóteses de interceptação de comunicações telemáticas (STF, 2006).

Não obstante, o Superior Tribunal de Justiça, em decisão proferida pela Quinta Turma, tem admitido o acesso a agendas telefônicas sem ordem judicial, sob o fundamento de que se trata de funcionalidade ordinária dos aparelhos celulares modernos, não gozando, portanto, da proteção conferida ao sigilo telefônico ou aos dados telemáticos.(STJ,2020).

Tal posicionamento, contudo, é alvo de críticas na doutrina, para a qual informações armazenadas, como fotografias, vídeos, históricos de navegação e registros de ligações, integram o núcleo essencial da privacidade e merecem proteção equivalente (Zilli, 2018, *apud* Smanio;Kibrit; Manhoso, 2023). Dessa forma, ainda que se mantenha a diferenciação entre dados protegidos pelo sigilo das comunicações e aqueles resguardados apenas pela privacidade, revela-se necessária uma disciplina normativa específica para este último grupo, a fim de definir com clareza os limites de acesso pelas autoridades e os critérios de sua utilização no processo penal.

De todo modo, qualquer restrição ao direito à intimidade e à vida privada deve observar estritamente os parâmetros constitucionais e submeter-se ao postulado da proporcionalidade, entendido, segundo Alexy (2001), em suas três dimensões: adequação, necessidade e proporcionalidade em sentido estrito. A medida restritiva deve, primeiramente, visar a um fim legítimo (adequação); em seguida, representar a alternativa menos gravosa entre as disponíveis (necessidade); e, por fim, oferecer benefícios que superem os prejuízos causados ao direito fundamental atingido (proporcionalidade estrita).

Cumpre salientar que, embora revestidos de inegável relevância, os direitos fundamentais não possuem caráter absoluto. Em situações excepcionais, podem ceder diante de outros valores constitucionais de igual estatura, como a preservação da ordem pública e a repressão à criminalidade, desde que observados

requisitos estritos de legalidade, proporcionalidade e reserva de jurisdição. Essa ponderação, como destaca Canotilho (2003,*apud* Smanio;Kibrit; Manhoso,2023), implica reconhecer que determinadas matérias, especialmente aquelas que envolvem restrições significativas a liberdades individuais, devem ser submetidas ao crivo prévio e fundamentado do Poder Judiciário, que atua como guardião da liberdade.

Não se pode, portanto, permitir que a proteção aos direitos fundamentais inviabilize por completo a persecução penal, sobretudo em hipóteses em que a investigação exige, de forma legítima, incursões mais profundas na esfera íntima do investigado, desde que dentro dos marcos constitucionais.

À luz do exposto, constata-se que alcançar o equilíbrio entre a eficiência investigativa e a proteção aos direitos à intimidade e à vida privada não é tarefa impossível, mas exige a implementação de regulamentação legislativa específica para os dados tutelados por tais direitos, com critérios objetivos e bem definidos,lacuna ainda existente no ordenamento jurídico. Não obstante, é plenamente possível que a atuação jurisdicional, ao apreciar a admissibilidade dessas provas ou ao autorizar sua obtenção, seja exercida de forma devidamente fundamentada, observando-se os parâmetros da adequação, da necessidade e da proporcionalidade, de modo a assegurar a legitimidade da medida e a preservação das garantias constitucionais.

2.4.2. Inviolabilidade do sigilo das comunicações

No tocante ao direito ao sigilo das comunicações, este encontra-se previsto no art. 5º, XII, da Constituição Federal, cuja redação dispõe:

> “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” (BRASIL, 1988).

Tal dispositivo consagra um direito fundamental destinado a resguardar o conteúdo das comunicações contra a ingerência estatal ou de terceiros não autorizados, constituindo dimensão essencial da privacidade e da liberdade individual. Como leciona Novelino (2010, p. 417), a finalidade dessa proteção é

impedir que a mensagem transmitida seja exposta a quem não figure como destinatário, frustrando, assim, a vontade do emissor em restringir seu conteúdo ao receptor escolhido.

O alcance dessa proteção constitucional foi complementado pela Lei nº 9.296/1996, que regulamenta a interceptação das comunicações telefônicas e telemáticas, fixando que tal medida somente pode ser autorizada por ordem judicial, em decisão fundamentada, quando houver indícios razoáveis de autoria ou participação em infração penal punida com reclusão, e a prova não puder ser obtida por outros meios.

No campo digital, essas diretrizes são reforçadas pelo Marco Civil da Internet (Lei nº 12.965/2014), cujo art. 7º, II, e §3º, assegura a inviolabilidade e o sigilo do fluxo de comunicações pela internet, permitindo seu afastamento apenas mediante ordem judicial, com procedimento formal e devidamente fundamentado.

No entanto, como observa Motta (2019), ainda que o Marco Civil da Internet discipline a proteção de comunicações e dados no ambiente digital, a referida lei não definiu regras próprias ou limites específicos aplicáveis à obtenção do conteúdo dessas comunicações. Por isso, parcela considerável da doutrina tem entendido que a quebra da inviolabilidade do sigilo, mesmo no contexto digital, deve seguir o regime da Lei nº 9.296/1996, aplicando-se, por analogia e interpretação extensiva, suas disposições às comunicações virtuais realizadas por meio de equipamentos, acessórios e aplicativos conectados à internet.

Nesse contexto, cumpre destacar a distinção, já delineada em tópico anterior, entre dados em trânsito,protegidos pelo art. 5º, XII, da CF, e dados estáticos, armazenados em dispositivos eletrônicos, cuja tutela se insere no art. 5º, X, da CF, como expressão da privacidade e da intimidade. Os primeiros correspondem às comunicações em fluxo, sujeitas à disciplina da interceptação, enquanto os segundos abrangem informações como fotografias, vídeos, registros de ligações e agendas de contatos, cujo acesso, embora também dependa de autorização judicial, segue regime jurídico distinto.

A jurisprudência tem reafirmado essa diferenciação, como no RMS 61.302/RJ (STJ, 2020), no qual se assentou que a quebra de sigilo de dados

estáticos relacionados à identificação de usuários, delimitada por parâmetros de tempo e local, não é desproporcional quando necessária à apuração de crimes graves. Faz-se importante ressaltar, contudo, que, como advertem Smanio, Kibrit e Manhoso (2023), essa diferenciação não pode ser utilizada como pretexto para fragilizar a proteção conferida aos dados pessoais, sob pena de esvaziar a eficácia do núcleo essencial do direito fundamental à privacidade e à intimidade.

Ademais, no âmbito das comunicações virtuais, a criptografia de ponta a ponta utilizada em aplicativos como o WhatsApp tem imposto obstáculos técnicos à interceptação direta, o que levou ao reconhecimento, pela jurisprudência, da possibilidade do espelhamento via WhatsApp Web como meio legítimo de obtenção de prova. No julgamento do Superior Tribunal de Justiça (STJ, 2024), entendeu-se que tal modalidade de monitoramento se equipara à infiltração de agente, prevista na Lei nº 12.850/2013, devendo seguir suas regras e ser utilizada apenas em hipóteses excepcionais, quando inexistirem meios menos invasivos para a investigação, e mediante autorização judicial.

Seguindo esse pressuposto, a jurisprudência também tem admitido, em casos de criminalidade organizada e delitos de alta complexidade, a conjugação da Lei nº 9.296/1996 com a Lei nº 12.850/2013, permitindo ações controladas e infiltrações no ambiente virtual, inclusive com acompanhamento em tempo real das comunicações interceptadas e espelhadas. No precedente analisado (STJ, 2023), destacou-se que essa interpretação busca compatibilizar a efetividade da persecução penal com a proteção das garantias fundamentais, reconhecendo que, em certas circunstâncias, a atuação investigativa deve adaptar-se às especificidades da criminalidade contemporânea, sem perder de vista os limites constitucionais.

Entretanto, o uso do espelhamento de WhatsApp como uma “infiltração virtual” não exime os investigadores de realizarem registro documental sobre o modo de coleta e preservação dos equipamentos, indicando quem teve contato com eles, quando tais contatos aconteceram e qual o trajeto administrativo interno percorrido pelos aparelhos uma vez apreendidos pela polícia, sendo necessário também informar o contexto em que se deu a breve apreensão (Assumpção, 2024).

Isso porque, a restrição ao sigilo das comunicações e de dados, por implicar severa limitação de direitos fundamentais, deve ser sempre excepcional e estritamente necessária. Capez (2017, *apud* Motta, 2019) adverte que tais medidas somente se justificam quando não houver outros meios menos lesivos capazes de produzir a prova necessária, incumbindo ao magistrado, no caso concreto, analisar a pertinência, a adequação e a necessidade da medida, fundamentando de forma clara sua decisão.

Diante disso, pode-se afirmar que a relativização do sigilo das comunicações, embora admitida no ordenamento jurídico, encontra-se condicionada ao cumprimento de requisitos constitucionais e processuais estritos. A doutrina majoritária e a jurisprudência consolidada indicam como pressupostos para a validade da medida: (i) previsão legal específica; (ii) ordem judicial fundamentada; (iii) delimitação objetiva do alcance da medida quanto ao conteúdo e ao período de coleta; (iv) indispensabilidade da prova; e (v) observância da cadeia de custódia, para assegurar a integridade e a autenticidade do material (Oliveira, 2021).

A observância desses limites cumpre dupla função: de um lado, legitima a atuação estatal, garantindo que a investigação se desenvolva dentro dos marcos constitucionais; de outro, preserva a validade e a admissibilidade da prova digital, evitando que sua obtenção por meios ilícitos ou abusivos comprometa todo o processo. Em última análise, trata-se de harmonizar o dever de repressão à criminalidade com a salvaguarda das liberdades individuais, reconhecendo que, embora o sigilo das comunicações e a proteção de dados sejam direitos fundamentais de elevada importância, não ostentam caráter absoluto, podendo ceder, de forma excepcional e proporcional, diante de necessidades legítimas da persecução penal.

2.4.3 Inadmissibilidade das provas ilícitas

A Constituição Federal, em seu art. 5º, inciso LVI, estabelece, de forma categórica, que “são inadmissíveis, no processo, as provas obtidas por meios ilícitos”. No plano infraconstitucional, o art. 157 do Código de Processo Penal, com redação dada pela Lei nº 11.690/2008, reforça essa diretriz, definindo como ilícitas as provas obtidas em violação a normas constitucionais ou legais, determinando seu desentranhamento dos autos.

Trata-se de garantia fundamental inserida no devido processo legal, voltada a impedir que a persecução penal se desenvolva à custa de violações a direitos e garantias individuais, preservando a legitimidade do sistema de justiça (Smanio, 2022).

No campo doutrinário, é importante diferenciar provas ilícitas de provas ilegítimas. As primeiras consistem naquelas obtidas mediante violação a normas de direito material ou a preceitos constitucionais, normalmente durante a fase investigativa ou em momento anterior à judicialização, como na hipótese de interceptação de comunicações sem autorização judicial. Já as provas ilegítimas decorrem da inobservância de normas de direito processual penal durante a produção da prova no curso do processo, como, por exemplo, a juntada intempestiva de documentos ou a realização de perícia sem a observância do contraditório. Enquanto a ilicitude contamina o próprio conteúdo probatório, acarretando sua inadmissibilidade e desentranhamento, a ilegitimidade conduz à nulidade do ato, com possibilidade de renovação válida (Lopes, 2025).

Não obstante a clareza do texto constitucional, a doutrina não é uníssona quanto ao alcance absoluto dessa vedação. Existem posições minoritárias que defendem, de um lado, a admissibilidade de provas ilícitas sempre que não se tratar de modalidade expressamente vedada no ordenamento, e, de outro, a absoluta proibição de seu uso, independentemente do contexto. Ambas as correntes, por penderem para extremos, não encontram acolhida majoritária.

Em contraposição, parcela expressiva da doutrina admite a flexibilização da regra por meio da aplicação dos princípios da proporcionalidade e da razoabilidade, autorizando o uso da prova ilícita quando indispensável à tutela de outro direito fundamental de igual ou maior relevância. Aury Lopes Jr. (2025) alerta, contudo, para o risco dessa construção, advertindo que a noção de proporcionalidade pode ser manipulada de forma a justificar restrições indevidas, especialmente quando se adota uma visão simplista de prevalência genérica do “interesse público” sobre o “interesse privado”.

Seguindo essa perspectiva, alguns autores admitem a utilização de provas ilícitas pro reo, argumentando que a condenação de um inocente

representaria dano mais grave do que a quebra de procedimentos formais, de modo que, nesse caso, seria legítimo sacrificar-se a regra para resguardar o direito fundamental à liberdade. Em sentido diverso, a aceitação pro societate,para assegurar a punição do culpado, é mais controvertida, mas há quem, como Norberto Avena (2023), sustente que, diante da atuação de organizações criminosas sofisticadas, não se deve restringir a proporcionalidade exclusivamente à proteção do réu, sob pena de inviabilizar a efetividade da persecução penal.

A inadmissibilidade das provas ilícitas se projeta também sobre aquelas que delas derivam, em aplicação da teoria dos frutos da árvore envenenada (*fruit of the poisonous tree doctrine*), positivada no art. 157, §1º, do CPP. Por essa construção, qualquer elemento probatório obtido a partir de uma prova ilícita é igualmente contaminado e, portanto, inadmissível. Capez (2024) pondera, entretanto, que não se pode adotar uma postura inflexível, pois, em determinadas hipóteses, o interesse protegido pode ser mais relevante do que o direito violado, sendo necessária a ponderação entre os princípios constitucionais em conflito.

Como resposta às limitações excessivas dessa doutrina, surgiram teorias que funcionam como exceções à inadmissibilidade por derivação. A primeira é a teoria da fonte independente, prevista expressamente no art. 157, §1º, do CPP, segundo a qual a prova será válida se puder ser obtida por um meio autônomo e lícito, sem nexo causal com a prova ilícita originária. A segunda é a teoria da descoberta inevitável, que admite a prova quando se demonstrar, com base em elementos concretos e verificáveis, que sua obtenção ocorreria de qualquer forma, por meios lícitos, ainda que inicialmente tenha sido encontrada de maneira ilícita (Lima, 2022).

No contexto das provas digitais, a aplicação dessas teorias exige cautela redobrada. Isso porque, a violação de direitos como o sigilo das comunicações e a privacidade,examinados nos subtópicos anteriores, cujos contornos e limites ainda não se encontram plenamente definidos no âmbito digital, bem como o descumprimento dos ritos da cadeia de custódia, podem conduzir à ilicitude probatória e contaminar a investigação subsequente. Em contrapartida, a constatação de que determinado dado poderia ser recuperado por perícia legítima

em cópia forense regularmente apreendida, ou que seria inevitavelmente identificado a partir de investigações paralelas, pode afastar a contaminação derivada.

Ante o exposto, é possível concluir que a discussão sobre a admissibilidade excepcional de provas ilícitas, especialmente no ambiente digital, converge para a necessidade de ponderação criteriosa pelo magistrado, à luz dos princípios da proporcionalidade e da razoabilidade. Tal ponderação, no entanto, deve ser conduzida com rigor metodológico, evitando interpretações que desvirtuem as garantias processuais e assegurando que a persecução penal, mesmo diante da gravidade dos crimes investigados, se mantenha compatível com os valores constitucionais que sustentam o Estado Democrático de Direito.

3. *FISHING* EXPEDITION: A VEDAÇÃO À BUSCA PROBATÓRIA GENERALIZADA

O terceiro capítulo da fundamentação teórica é dedicado à análise aprofundada do fenômeno denominado *fishing expedition*, expressão que, no campo jurídico, designa a busca probatória genérica, ampla e desvinculada de parâmetros objetivos, configurando verdadeira “pescaria” indiscriminada de informações.

A priori, examina-se a origem do termo, seu conceito e a forma como tem sido aplicado no processo penal brasileiro, com o intuito de delimitar os elementos que caracterizam uma busca predatória e compreender os critérios doutrinários e jurisprudenciais utilizados para identificar tal prática. Busca-se, assim, estabelecer os contornos teóricos que permitam diferenciar a atuação legítima de investigação daquela que se converte em exploração probatória arbitrária.

Em seguida, o estudo se volta para a manifestação dessa prática no ambiente digital, especialmente nas interceptações telemáticas, nas buscas e apreensões de aparelhos celulares e no acesso remoto a dados por meio de *malwares*. Isso porque os riscos de ilegalidade nesse contexto mostram-se ainda mais acentuados, considerando que a concentração massiva de informações pessoais em dispositivos eletrônicos, aliada à facilidade e rapidez no seu acesso,

amplia a possibilidade de devassas indevidas e dificulta a delimitação precisa do que efetivamente será objeto de análise.

Por fim, analisa-se a colisão entre a prática do *fishing expedition* e os direitos e garantias fundamentais, evidenciando que a adoção de diligências especulativas e sem causa provável afronta pilares do processo penal democrático, como a presunção de inocência, a garantia contra a autoincriminação e o direito à intimidade e à privacidade. Demonstra-se, nesse ponto, que as provas colhidas por meio de tais expedientes devem ser qualificadas como ilícitas, em razão da violação direta ao devido processo legal e às balizas constitucionais da atividade probatória.

Nesse sentido, o presente capítulo contribui para o aprofundamento do debate acerca da admissibilidade das provas digitais, evidenciando que o *fishing expedition* representa uma das principais causas de ilicitude probatória no meio eletrônico. Essa discussão prepara o terreno para o capítulo subsequente, no qual se examinará a serendipidade no âmbito digital, fenômeno que, embora também relacionado à descoberta de provas em contexto diverso do originalmente autorizado, apresenta contornos e implicações distintas.

3.1 Origem e conceito do termo *"fishing expedition"*

Antes de adentrar propriamente no conceito e nas peculiaridades do fenômeno denominado *fishing expedition*, ou "pescaria probatória", faz-se oportuno resgatar brevemente sua origem histórica e o contexto jurídico em que se desenvolveu.

Nos países adeptos do sistema *common law*, especialmente entre o final do século XVIII e o início do século XIX, registraram-se mudanças significativas nas possibilidades de defesa do acusado, marcadas pela consolidação da presunção de inocência e pela introdução do critério da dúvida razoável. Essas garantias impuseram limites mais rigorosos às práticas processuais voltadas à obtenção de provas, coibindo expedientes que desvirtuassem a finalidade do processo penal. Nesse cenário, ganharam destaque procedimentos que criavam verdadeiras "redes" de colheita de informações, capazes de capturar dados de forma especulativa e

indiscriminada ,prática que passou a ser denominada *fishing expedition* (Molina, 2020, *apud* Batista; Filho, 2022).

Seguindo esse pressuposto, verifica-se que o termo tem origem no direito estadunidense, inserido no contexto do modelo jurídico do *common law*, que apresenta características substancialmente distintas do sistema de *civil law* adotado no Brasil.

No ordenamento norte-americano, o processo judicial divide-se, de modo geral, em duas fases: o *pretrial* (momento anterior ao julgamento) e o *trial* (fase de julgamento, que, em causas cíveis ou criminais, pode ser realizado por um júri). A etapa do *pretrial* contempla o chamado *discovery*, procedimento destinado à revelação de provas e dados relevantes para a elucidação do caso. Nessa fase, não há participação direta do magistrado na condução dos atos probatórios, cabendo principalmente aos advogados a produção de provas, com a supervisão formal de um oficial de cartório, que atua como representante do juízo (Cambi; Pitta, 2015).

Foi nesse contexto que a expressão *fishing expedition* se consolidou para designar situações em que uma das partes se vale dos instrumentos processuais disponíveis para buscar, de forma genérica e desvinculada de pertinência temática, informações que possam, de algum modo, incriminar a parte contrária, mesmo que tais informações não guardem relação direta com o objeto da ação. Segundo Pitta (2019), trata-se da utilização de meios probatórios “com a intenção de localizar dados que, a princípio, não seriam considerados relevantes para o julgamento”.

De forma semelhante, o dicionário Merriam-Webster (2025) define *fishing expedition* como: “(1) investigação desnecessariamente extensa ou irrelevante para o processo; (2) investigação que não atende ao objetivo declarado, mas que visa descobrir provas incriminatórias ou dignas de divulgação”.

Embora inicialmente identificado no campo das ações cíveis, o termo passou a ser amplamente utilizado no processo penal, inclusive em recentes decisões e estudos relacionados ao sistema brasileiro. A tradução literal da expressão para o português — “expedição de pesca” — evoca a imagem de quem lança redes ou anzóis em águas desconhecidas, sem qualquer conhecimento prévio sobre o que se encontrará. Trata-se de uma busca guiada mais pela tentativa e erro

do que por um objetivo claro, na qual se varre uma área ampla na esperança de capturar algo de interesse.

Em termos jurídicos, essa analogia descreve a atuação de autoridades que, desprovidas de um escopo probatório bem definido, realizam buscas amplas e indiscriminadas na expectativa de encontrar elementos incriminadores, ainda que sem relação direta e comprovada com o fato investigado.

Nesse cenário, um dos mais relevantes trabalhos sobre o tema, desenvolvido por Alexandre Morais da Rosa, Viviani Ghizoni Silva e Philipe Benoni Melo e Silva, conceitua a *fishing expedition* nos seguintes termos:

> "investigação especulativa indiscriminada, sem objetivo certo ou declarado, que 'lança' suas redes com a esperança de 'pescar' qualquer prova, para subsidiar uma futura acusação. Ou seja, é uma investigação prévia, realizada de maneira muito ampla e genérica para buscar evidências sobre a prática de futuros crimes. Como consequência, não pode ser aceita no ordenamento jurídico brasileiro, sob pena de malferimento das balizas de um processo penal democrático de índole Constitucional"(Rosa;Silva;Melo e Silva, 2019)

Ainda segundo Alexandre Morais da Rosa (2021), a expressão remete à incerteza inerente às expedições de pesca, nas quais não se sabe, previamente, se haverá peixe, quais espécies serão fisgadas ou em que quantidade, mas se alimenta uma “convicção” de que algo será encontrado. Com o uso intensivo de tecnologia no contexto do chamado Processo Penal 4.0, essa prática tem potencializado a obtenção de provas por meios escusos,como investigações paralelas não autorizadas, aproveitamento de elementos colhidos de forma irregular e uso dissimulado do “encontro fortuito”, afastando-se do controle jurisdicional e das garantias democráticas.

Assim, como observa Aury Lopes Jr. (2025), a *fishing expedition* representa um indevido aproveitamento do espaço de poder conferido ao aparato investigatório estatal para subverter a lógica do devido processo legal, invadindo a intimidade, a vida privada, o sigilo de dados e a inviolabilidade domiciliar em busca de qualquer elemento incriminador, mesmo que alheio à causa originária da investigação.

Dessa forma, a ausência de objetividade na definição do escopo da diligência e a adoção de um alvo excessivamente amplo configuram marcas desse fenômeno, que pode se manifestar em diferentes meios de obtenção de prova,desde buscas e apreensões domiciliares ou pessoais, interceptações telefônicas e telemáticas, até a coleta de dados digitais. Essas hipóteses serão examinadas no subtópico seguinte, à luz do modelo processual penal acusatório brasileiro e das garantias fundamentais dos investigados.

3.2. Hipóteses de ocorrência no ambiente digital

No intuito de compreender a materialização do *fishing expedition* no âmbito digital e sua consequente colisão com os direitos e garantias fundamentais, faz-se necessário elencar as hipóteses típicas em que tal prática se manifesta.

A esse respeito, Rosa (2021) dispõe que:

> "A criatividade dos agentes públicos oportunistas no 'aproveitamento' de diligências, com ou sem autorização para colocar em prática a expedição probatória pode-se configurar, dentre outras hipóteses: a) busca e apreensão sem alvo definido, tangível e descrito no mandado (mandados genéricos); b) vasculhamento de todo o conteúdo do celular apreendido; c) continuidade da busca e apreensão depois de obtido o material objeto da diligência; d) investigações criminais dissimuladas de fiscalizações de órgãos públicos; e) interceptação e monitoramento por períodos longos de tempo; f) prisão temporária ou preventiva para 'forçar' a descoberta ou colaboração premiada ou incriminação; g) buscas pessoais (ou residenciais) desprovidas de 'fundada suspeita' prévia e objetiva; h) quebra de sigilo (bancário, fiscal, dados etc.) sem justificativa do período requisitado."

Dentre essas hipóteses, destacam-se, para os fins do presente estudo: a busca e apreensão sem alvo definido, tangível e descrito no mandado; o vasculhamento integral de todo o conteúdo de celular apreendido e a interceptação e monitoramento prolongados.

No que concerne à busca e apreensão, o art. 243 do Código de Processo Penal dispõe que o mandado deve indicar, "o mais precisamente possível", o local da diligência, o nome do respectivo proprietário ou morador e a motivação e finalidade da medida, estruturando critérios que visam coibir diligências genéricas.

No âmbito digital, contudo, a busca e apreensão de dispositivos eletrônicos não conta com regramento específico, aplicando-se as disposições previstas para objetos físicos. Essa equiparação, todavia, ignora que os dados digitais concentram milhares de informações interligadas, ampliando de forma desproporcional a restrição aos direitos fundamentais.

Conforme apontam Saad, Rossi e Partata (2024), diferentemente do espaço físico de uma residência, que possui limites definidos, um dispositivo eletrônico pode armazenar volume incomparavelmente maior de dados, superando em muito os contornos da busca física. Além disso, enquanto no mundo físico normalmente se busca e, em seguida, se apreende o que é relevante, no ambiente digital observa-se, com frequência, a coleta indiscriminada de todo o conteúdo, para só depois filtrar o que interessa à investigação.

Essa necessidade de cautela é reforçada por Greco e Gleizer (2019), que destacam que os celulares acompanham seus usuários em todos os ambientes, armazenando não apenas mensagens e e-mails, mas também registros de áudio e vídeo que podem incluir relações sexuais, discussões íntimas, consultas médicas ou diálogos com advogados. O acesso irrestrito a tais conteúdos ameaça não apenas o núcleo essencial da privacidade, mas também a própria confiança no uso de dispositivos informáticos, que podem ser transformados em instrumentos de vigilância ambiental.

De tal modo, com base na jurisprudência já examinada em subtópicos anteriores, conclui-se que a autorização judicial para acesso a dispositivos apreendidos não é apenas necessária, mas indispensável, devendo vir acompanhada de fundamentação clara e objetiva.

Não obstante, o Supremo Tribunal Federal, em recente decisão (2025), admitiu a possibilidade de acesso, pela autoridade policial, a aparelho eletrônico encontrado fortuitamente em local vinculado ao fato delituoso, sem prévia autorização judicial, desde que tal diligência se restrinja à identificação do proprietário ou da autoria do crime.

Neste ponto, à luz das considerações acerca da pescaria probatória, impõe-se reconhecer que tal hipótese apresenta elevado potencial de

desvirtuamento. Questiona-se, portanto, até que ponto essa atuação, na prática, permanecerá efetivamente limitada a essa finalidade específica. Isso porque, embora a medida possua escopo restrito, a experiência demonstra que, uma vez franqueado o acesso ao aparelho, a tênue linha que separa a diligência legítima de uma busca predatória e indiscriminada, apta a alcançar dados e informações inteiramente alheios ao objeto inicial da investigação, pode ser facilmente ultrapassada.

Assim como ocorre na busca e apreensão sem alvo definido, o *fishing expedition* também se manifesta no vasculhamento integral de dispositivos eletrônicos, prática observada tanto em mandados genéricos, pela falta de especificidade quanto ao que se busca, quanto na continuidade da diligência após já ter sido obtido o material de interesse.Nesse mesmo contexto, o acesso remoto e oculto a dispositivos por meio de *malwares* ou técnicas de hacking estatal revela-se igualmente propício à prática da pesca probatória, pois possibilita o acompanhamento constante e inadvertido das informações armazenadas e geradas pelo usuário, permitindo a devassa de dados pessoais sem que haja ciência do investigado ou mesmo conhecimento do próprio Poder Judiciário, em nome da preservação da eficácia da medida.

Essa hipótese foi enfrentada de forma paradigmática pelo Supremo Tribunal Federal no Inquérito nº 4.831/DF, no qual o ministro Celso de Mello limitou o alcance da perícia solicitada pela Procuradoria-Geral da República sobre dados do celular do ex-Ministro Sérgio Moro, para impedir que a medida assumisse caráter exploratório:

> “Se tornará necessário identificar, se possível, os interlocutores dos diálogos mantidos pelo Senhor Sérgio Moro que serão objeto do exame pericial ora pretendido, definindo-se, ainda, o espaço temporal em que esses elementos de informação deverão ser coligidos, **respeitando-se, sempre, a necessária vinculação com os fatos objeto deste inquérito das mensagens de texto e áudio, imagens e vídeos armazenados em aludido aparelho de telefonia celular, para que tal diligência investigatória não se converta, indevidamente, em instrumento de indiscriminada e inaceitável devassa estatal**. E o motivo de observar-se a existência de conexão com os eventos alegadamente delituosos sob investigação penal reside no fato de que **o nosso sistema jurídico, além de amparar o princípio**

> **constitucional da intimidade pessoal, repele atividades probatórias que caracterizem verdadeiras e lesivas 'fishing expeditions', vale dizer, o ordenamento positivo brasileiro repudia medidas de obtenção de prova que se traduzam em ilícitas investigações meramente especulativas ou randômicas, de caráter exploratório, também conhecidas como diligências de prospecção**, simplesmente vedadas pelo ordenamento jurídico brasileiro." (STF, Inq 4.831/DF, Rel. Min. Celso de Mello, julgado em 05/05/2020).(grifo nosso)

Outra hipótese relevante é a interceptação e o monitoramento por períodos longos de tempo, sem justificativa do período requisitado, o que impacta diretamente o direito fundamental ao sigilo das comunicações. Embora seja medida de reconhecida eficácia no combate à criminalidade, a interceptação deve observar os requisitos da Lei nº 9.296/1996, entre eles a presença de indícios razoáveis de crime punido com reclusão e a impossibilidade de obtenção da prova por outros meios.

Quanto à questão temporal,o art. 5º desta lei prevê prazo inicial de quinze dias, prorrogável enquanto presentes os pressupostos. Entretanto, o Superior Tribunal de Justiça já decidiu que a prorrogação somente é válida se fundamentada, ainda que de forma sucinta, com base na necessidade da medida e na complexidade do caso. No AgRg no HC 910.860/PB, a Sexta Turma considerou inválidas as prorrogações que apenas repetiam fundamentos da decisão inicial, sem análise específica de cada pedido, por configurarem fundamentação genérica. Concluiu-se que o magistrado deve motivar cada renovação a partir da situação concreta existente no momento da decisão, não sendo suficiente mera remissão à decisão inaugural (STJ, 2024).

Diante do exposto, constata-se que o fenômeno do *fishing expedition* pode manifestar-se em múltiplas circunstâncias, assumindo contornos particularmente sensíveis no ambiente digital, onde a amplitude e a natureza das informações acessadas potencializam seus riscos. Tal realidade impõe especial atenção aos direitos e garantias fundamentais comprometidos pela prática, notadamente os princípios da presunção de inocência e da não autoincriminação, cuja análise será objeto do subtópico seguinte.

3.3 A colisão com os direitos e garantias fundamentais e a ilicitude das provas obtidas

Tendo em vista o conceito e as hipóteses de materialização do *fishing expedition*, cumpre situá-lo no processo penal brasileiro. Como já consignado, o modelo vigente é essencialmente acusatório, com nítida separação das funções de acusar, defender e julgar, vedação à iniciativa probatória do magistrado e centralidade da presunção de inocência, que impõe à acusação o ônus de demonstrar a culpabilidade além de dúvida razoável, tudo sob a égide da publicidade, do contraditório e da ampla defesa.

Diante desse panorama, admitir a prática da pesca probatória seria manifestamente contraditório, uma vez que afronta diversos direitos e garantias fundamentais. Entre eles, destacam-se a presunção de inocência, o direito à não autoincriminação e, de forma inequívoca, os direitos à intimidade, à privacidade e ao sigilo das comunicações e dos dados.

No que se refere à presunção de inocência, prevista no art. 5º, LVII, da Constituição Federal e no art. 8.2 da Convenção Americana de Direitos Humanos (Brasil, 1969), trata-se do direito de não ser considerado culpado senão após o trânsito em julgado de sentença penal condenatória ou enquanto não for legalmente comprovada sua culpa, conforme a convenção. Acerca da “comprovação legal”, entende-se que ocorre apenas com o esgotamento do duplo grau de jurisdição, ou seja, após a confirmação da sentença condenatória pelo órgão ad quem.

A doutrina majoritária identifica duas dimensões do princípio: a regra de tratamento, que impõe ao Estado a obrigação de considerar o acusado como inocente até decisão condenatória definitiva, e a regra probatória, que atribui ao órgão acusador o ônus de demonstrar a culpabilidade do réu além de dúvida razoável (Lima, 2022).

Nesse horizonte, diligências aleatórias e especulativas, orientadas a “pescar” qualquer elemento incriminatório, desvirtuam a lógica do processo penal democrático. Isso porque, em vez de investigar um fato objetivamente delimitado, com causa provável e finalidade definida, a pescaria probatória transforma o

investigado em alvo permanente de devassas, inverte o ônus da prova e normaliza a busca por confirmações *ex post* de uma suspeita não demonstrada. O resultado é uma presunção às avessas: parte-se do pressuposto de culpa para vasculhar a vida do indivíduo em busca de algo que corrobore essa narrativa, o que afronta, de maneira direta, a presunção de inocência e a regra probatória que dela emana.

De modo correlato, a garantia contra a autoincriminação (*nemo tenetur se detegere*), prevista no art. 5º, LXIII, assegura ao acusado o direito de não produzir prova contra si mesmo, inclusive por meio do silêncio. Como observa Renato Brasileiro (2022), não se pode exigir comportamento ativo do investigado quando isso possa conduzir à sua própria incriminação. Em diligências especulativas, sobretudo no ambiente digital, essa proteção é vulnerada por vias oblíquas: o indivíduo, muitas vezes sem ciência de estar sob escrutínio, produz provas contra si de forma involuntária, deixando traços, registros e metadados que são convertidos em reforços probatórios sem que tenha havido provocação legítima ou delimitação prévia da medida.

A vedação à pescaria probatória revela-se, por isso mesmo, corolário lógico do *nemo tenetur*: diligências sem causa provável e sem objeto definido terminam por impor autoincriminação indireta, incompatível com a matriz garantista do processo penal (Rosa, 2021).

A vulnerabilidade se agrava quando a investigação recorre a expedientes intensamente intrusivos sobre a vida informacional do investigado. Matos (2022) observa que o direito de não se autoincriminar é particularmente suscetível quando se colhem elementos de dispositivos eletrônicos pessoais, nos quais se armazenam, sem advertência prévia sobre a possível flexibilização de garantias, dados íntimos do próprio investigado e de terceiros.

Mendes (2020) acrescenta que, por desconhecerem a técnica investigativa empregada, “os indivíduos-alvos continuam a agir, em um sentido claramente auto incriminatório ou incriminatório daqueles com os quais interagem”, expondo manifestações não livres nem esclarecidas que, mais tarde, poderão ser utilizadas contra eles em juízo. Em outras palavras, a amplitude indeterminada da

diligência converte a rotina digital do cidadão em fonte de prova contra si, sem o controle material que a Constituição exige.

Essa tensão evidencia a constante tentativa de equilíbrio entre direitos fundamentais do investigado e o interesse público na persecução penal. Como lembra Queijo (2013), se os direitos do réu fossem reconhecidos em caráter absoluto, inviabilizar-se-ia a repressão penal; na direção oposta, se o interesse público prevalecesse de forma ilimitada, qualquer abuso poderia ser legitimado em nome da busca da chamada “verdade real”, o que se mostra inconciliável com um Estado Democrático de Direito. Daí decorre a necessidade de observar os critérios de adequação, necessidade e proporcionalidade, parâmetros que não se verificam nas hipóteses de materialização do *fishing expedition*.

Além disso, admitir a pescaria probatória no ambiente digital implicaria violação desmedida à intimidade, à vida privada e ao sigilo das comunicações e dos dados, direitos reforçados pela Emenda Constitucional nº 115/2022, que inseriu no art. 5º, LXXIX, a proteção de dados pessoais, inclusive nos meios digitais. O traço constitutivo do *fishing expedition* é a indeterminação, tendo em vista que o objeto é incerto, o resultado é aleatório e o caminho de coleta é aberto. Não há como compatibilizar esse modelo com um processo penal que só tolera restrições quando estritamente necessárias, proporcionais e legalmente fundamentadas.

Nesse cenário, a consequência jurídica é inequívoca. Provas obtidas por meio de pescaria probatória qualificam-se como ilícitas, por violarem direitos fundamentais e regramentos legais de obtenção e produção de prova, devendo ser inadmitidas e desentranhadas, com as repercussões próprias sobre os elementos derivados.

Não se trata de obstaculizar a persecução penal, mas de preservá-la dentro das “regras do jogo válido”, para evitar que o fim contamine os meios e deslegitime a resposta estatal. Nesse sentido, Aury Lopes Jr. ensina que:

> “Existem as regras do jogo, as regras do devido processo, que jamais podem ser desconsideradas, pois devemos garantir para punir e punir garantindo. Respeito aos direitos fundamentais não é sinônimo de impunidade. [...] Não se pune ilegalidades cometendo ilegalidades, não se combate crime cometendo crime. Essa é a síntese da equação punição–garantias fundamentais.”(Lopes,2025)

Dessa forma, como destaca Ramos (2022), o rechaço judicial a investigações especulativas cumpre não apenas uma função de proteção aos direitos fundamentais, mas também pedagógica e sistêmica, desestimulando práticas abusivas e reafirmando os limites constitucionais da atividade probatória.

Superadas essas considerações acerca do *fishing expedition* e da vedação à busca probatória generalizada, importa agora examinar outro fenômeno que se projeta no âmbito do processo penal digital: a serendipidade. Diferentemente da pescaria probatória, a serendipidade se refere à descoberta fortuita de elementos probatórios durante uma diligência legítima, o que impõe a necessidade de delimitar seus contornos, fundamentos e critérios de admissibilidade, a fim de distingui-la de práticas abusivas e compreender seus reflexos na persecução penal contemporânea.

4 A SERENDIPIDADE DIGITAL E A ADMISSIBILIDADE DA PROVA FORTUITA

Encerrado o exame do fenômeno do *fishing expedition*,cuja nota distintiva é a busca indiscriminada e aleatória de elementos probatórios em desconformidade com os limites constitucionais do processo penal, importa avançar para a análise de outro fenômeno que também se manifesta no processo penal contemporâneo: a serendipidade. Diferentemente da pescaria probatória, a serendipidade não resulta de uma devassa indiscriminada, mas da descoberta fortuita de elementos probatórios durante uma diligência legítima e previamente delimitada, o que lhe atribui contornos próprios.

Essa peculiaridade impõe a necessidade de examinar o fenômeno em profundidade, uma vez que o aproveitamento de provas obtidas de forma fortuita, se por um lado pode fortalecer a busca pela verdade, por outro suscita o risco de legitimar práticas abusivas quando não observado o devido processo legal. Assim, a serendipidade deve ser compreendida a partir de seus fundamentos, limites e critérios de validade, para que sua admissão não se converta em pretexto para autorizar expedientes incompatíveis com os direitos fundamentais.

O presente capítulo tem por finalidade delimitar o conceito e os fundamentos da serendipidade no processo penal, compreendendo-a como o achado probatório casual que emerge no curso de uma diligência legítima e previamente autorizada. A partir disso, examinar-se-ão os critérios de validade da prova fortuita em ambiente digital, tendo em vista as peculiaridades dos meios de obtenção de prova que incidem sobre dados armazenados em dispositivos eletrônicos ou transmitidos por redes telemáticas, nos quais o volume, a diversidade e a sensibilidade das informações aumentam exponencialmente os riscos de violação a direitos fundamentais.

Em seguida, será abordada a distinção entre serendipidade e *fishing expedition*, ponto crucial para a tese aqui defendida. Se, de um lado, a serendipidade é marcada pela casualidade e pela vinculação da descoberta a uma diligência legítima, de outro, a pesca probatória caracteriza-se pela indeterminação e pela especulação, de modo que diferenciar tais fenômenos é essencial para evitar que a prática abusiva se esconda sob a aparência de achado fortuito.

O estudo avançará, ainda, sobre os mandados judiciais genéricos e os limites da atuação estatal, visto que a falta de delimitação clara do objeto da medida investigativa compromete a linha tênue que separa a prova fortuita da prova ilícita. Nessa perspectiva, será analisado o papel da fundamentação judicial como instrumento de contenção de abusos e de garantia da legitimidade do processo penal.

A relevância deste capítulo reside, portanto, em completar a análise do eixo central do trabalho, contrapondo à vedação da pesca probatória a possibilidade, em situações específicas, de aproveitamento da prova fortuita descoberta em ambiente digital. Dessa forma, pretende-se oferecer uma reflexão sistemática sobre os limites constitucionais da admissibilidade da prova penal em tempos de intensa transformação tecnológica, concluindo a fundamentação teórica necessária ao enfrentamento da problemática proposta.

4.1 Origem e conceito de serendipidade

De início, faz-se relevante tratar da origem e do significado do termo *serendipidade*. A palavra decorre do substantivo inglês *serendipity*, que designa “a

faculdade ou fenômeno de encontrar coisas valiosas ou agradáveis não procuradas” (*the faculty or phenomenon of finding valuable or agreeable things not sought for*) (Merriam, 2025). No vernáculo português, o vocábulo pode ser conceituado como aquilo que acontece ou é descoberto por acaso, de forma imprevista e inesperada.

Nesse contexto, a gênese histórica da expressão remonta ao ano de 1754, quando o escritor inglês Horace Walpole cunhou o termo *serendipity* em referência ao conto persa “Os Três Príncipes de Serendip”, cuja narrativa descreve a realização de descobertas surpreendentes e não planejadas ao longo da jornada dos personagens (Capez, 2021).

Desde então, a palavra passou a ser associada a achados casuais dotados de relevância, extrapolando o campo literário para alcançar diversas áreas do conhecimento, inclusive o direito, e, em especial, o processo penal. No cenário brasileiro, o encontro fortuito de provas tornou-se objeto cada vez mais recorrente de debates doutrinários e jurisprudenciais, questionando-se, sobretudo, a possibilidade de aproveitamento de elementos probatórios surgidos no curso da investigação que não guardavam relação direta com o objeto inicialmente delimitado.

Como já se consignou, não encontra respaldo no ordenamento jurídico vigente a prática de diligências genéricas e indiscriminadas, carentes de alvo ou objeto definido. Todavia, pode ocorrer que, no cumprimento de medida cautelar regularmente autorizada e devidamente fundamentada, surjam elementos probatórios alheios ao escopo inicial da investigação. Nessas hipóteses, obtêm-se resultados que ultrapassam os limites originalmente fixados, situação que, a depender das circunstâncias, pode configurar tanto uma distorção da finalidade da medida quanto a ocorrência legítima do chamado encontro fortuito de provas.

A esse respeito, Renato Brasileiro leciona:

> A teoria do encontro fortuito ou casual de provas é utilizada nos casos em que, no cumprimento de uma diligência relativa a um delito, a autoridade policial casualmente encontra provas pertinentes à outra infração penal (crime achado), que não estavam na linha de desdobramento normal da investigação. Fala-se em encontro fortuito de provas ou serendipidade quando a prova de determinada infração penal é obtida a partir de diligência regularmente autorizada para a investigação de outro crime(Lima, 2022)

Na mesma direção, Alexandre Morais da Rosa observa que o encontro fortuito de provas ocorre “no curso do cumprimento ou execução de medida cautelar probatória, de elementos indicativos de crimes ou personagens não contidos na investigação originária” (Rosa, 2021).

Ainda, para boa parte da doutrina, como destaca Aury Lopes Jr. (2025), a temática insere-se no campo do desvio causal de prova e da prova emprestada, compartilhada ou transferida, hipótese em que determinada prova é colhida no contexto da apuração de um crime e, posteriormente, aproveitada em outro processo no qual também passa a ser valorada.

A título ilustrativo, pode-se mencionar que o encontro fortuito de provas ocorre, por exemplo, quando, no curso de interceptação telefônica regularmente autorizada para apuração de tráfico de drogas, revela-se a prática de um homicídio (Zimiani, 2020), ou, ainda, quando, durante o cumprimento de mandado de busca e apreensão, a autoridade policial se depara com indícios de infração penal distinta daquela que motivou a expedição da medida.

O termo *serendipidade* já foi empregado em diversas oportunidades pelo Supremo Tribunal Federal e pelo Superior Tribunal de Justiça, adquirindo, inclusive, contornos principiológicos no âmbito jurisprudencial. Todavia, a doutrina ainda diverge quanto aos requisitos para a admissibilidade da prova fortuita, notadamente sobre a necessidade de conexão entre os delitos ou da identidade dos sujeitos envolvidos no crime “achado”. Diante dessas divergências, o subtópico seguinte será destinado a examinar as principais posições doutrinárias e a aceitação da prova fortuita, de modo a estabelecer a base teórica indispensável para, posteriormente, avançar na análise de seus critérios de validade em ambiente digital.

4.2 Posições doutrinárias e aceitação da prova fortuita

A doutrina apresenta duas classificações relevantes acerca da serendipidade. A primeira distingue entre a serendipidade objetiva e a subjetiva; a segunda, entre a serendipidade de primeiro e de segundo grau.

Diz-se que a serendipidade subjetiva ocorre quando há surpresa em relação aos sujeitos do crime, isto é, quando no curso da investigação surgem

indícios acerca de outros agentes que não estavam compreendidos no desdobramento natural da diligência, constatando-se a coautoria ou a participação em concurso de pessoas em um delito diverso (Soares; Oliveira, 2023). Já a serendipidade objetiva se caracteriza quando o “crime achado” envolve os mesmos participantes do delito originalmente investigado, ainda que persista o elemento surpresa em relação aos novos fatos descobertos.

A serendipidade objetiva, por sua vez, divide-se em duas modalidades: de primeiro grau e de segundo grau. A primeira refere-se às hipóteses em que as provas ou delitos encontrados guardam relação de conexão com o objeto inicial da investigação, de modo que sua admissibilidade dependeria desse vínculo. De forma diversa, a serendipidade de segundo grau admite a utilização da prova fortuita ainda que não exista conexão entre os delitos, bastando a sua descoberta no curso de uma diligência legítima. Capez sintetiza a distinção da seguinte maneira:

> 1) Serendipidade de primeiro grau: exige nexo causal em relação ao crime investigado originariamente, como, por exemplo, a localização do cadáver ocultado, durante a apuração do respectivo homicídio;
> 2) Serendipidade de segundo grau: a prova descoberta fortuitamente será válida, independentemente de existir ou não conexão com o fato originalmente apurado. Nesse sentido, seria lícita a prova de roubo colhida fortuitamente em uma interceptação telefônica para investigação de estupro. (Capez, 2021)

A primeira posição, defendida por Aury Lopes Jr. (2025), sustenta que a admissibilidade da prova fortuita deve observar necessariamente um vínculo de conexão com o delito que justificou a medida originária. Isso porque a autorização judicial que sacrifica direitos fundamentais, como na hipótese de buscas domiciliares, quebras de sigilo bancário, fiscal ou telefônico, possui caráter excepcional e deve ser interpretada de forma estrita, vinculando-se à finalidade específica que legitimou sua concessão.

Nessa linha, a decisão judicial encontra-se, ao mesmo tempo, vinculada ao pedido formulado pelo órgão acusador e vinculante quanto ao material colhido, de modo que a utilização das provas deve permanecer restrita à apuração do crime que ensejou a autorização. Admitir seu aproveitamento irrestrito em outros

procedimentos, sem a necessária conexão, equivaleria a um desvio causal, transformando a prova em elemento ilícito por derivação e comprometendo a higidez do processo penal.

O autor destaca, ainda, a contradição inerente a esse aproveitamento: a prova seria ilícita e desprovida de valor no processo originário, mas, paradoxalmente, serviria de base como notícia-crime em outro procedimento. Tal postura, segundo Lopes Jr. (2025), afrontaria o princípio da legalidade, pois a investigação deve se iniciar a partir de prova lícita, sob pena de contaminação de todos os atos subsequentes da persecução penal.

Contudo, não obstante a relevância e a consistência dos argumentos apresentados, esse entendimento não corresponde à posição majoritária da doutrina, tampouco da jurisprudência, que têm se orientado por uma aceitação mais ampla da prova fortuita.

Seguindo essa linha, merece destaque o posicionamento do Supremo Tribunal Federal no julgamento do HC 129.678/SP (Brasil, 2017), no qual se discutiu a validade de prova obtida em contexto de interceptação telefônica. Na ocasião, o réu estava sendo investigado pelo crime de tráfico de drogas e, diante da presença dos requisitos constitucionais e legais, o magistrado deferiu a medida cautelar de interceptação das comunicações. Durante o monitoramento, contudo, foi revelado que o acusado também teria praticado crime de homicídio.

A questão central residia em saber se a prova referente ao homicídio poderia ser admitida, mesmo não guardando conexão direta com o tráfico de drogas, objeto da investigação inicial. Ao apreciar o caso, o ministro Alexandre de Moraes, redator para o acórdão, entendeu pela licitude do elemento probatório, destacando que se tratava do chamado “crime achado”, hipótese em que a infração penal não estava sob investigação até o momento em que, no curso de apuração legítima de outro fato, foi descoberta fortuitamente. Nas palavras do ministro:

> “Assim, o ‘crime achado’ – ou seja, a infração penal desconhecida e, portanto, até aquele momento não investigada – sempre deve ser cuidadosamente analisado para que não se relativize em excesso o inciso XII do art. 5º da Constituição (‘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'). Apesar de não haver dados nos autos que atestem se há ou não conexão entre os crimes, a prova obtida mediante interceptação telefônica quanto a essa infração penal diversa da investigada deve ser considerada lícita, pois presentes os requisitos constitucionais e legais: a interceptação foi autorizada por ordem judicial e o crime é apenado com reclusão. Só poderia ser afastada a prova se verificássemos – o que não é o caso – alguma hipótese de desvio de finalidade. Lamentavelmente, às vezes, isso ocorre nas investigações. Faz-se uma fraude para a obtenção da interceptação, para se investigar ilicitamente terceiros. Contudo, na espécie, trata-se do típico 'crime achado', que não constitui prova ilícita – havia autorização judicial, é bom repetir. Consequentemente, afasto, assim como Vossa Excelência, a ilicitude dessa prova." (STF,2017).

Em igual sentido, o Superior Tribunal de Justiça também já reconheceu a admissibilidade da prova fortuita em hipóteses semelhantes. No HC 187.189/SP (Brasil, 2013), a Corte entendeu pela legalidade da utilização de provas de crimes de lavagem de dinheiro e associação criminosa, descobertas fortuitamente durante interceptações telefônicas originalmente autorizadas para investigar delitos de contrabando e descaminho. Conforme consignado no voto vencedor:

> "É legítima a utilização de informações obtidas em interceptação telefônica para apurar conduta diversa daquela que originou a quebra de sigilo, desde que por meio dela se tenha descoberto fortuitamente a prática de outros delitos. Caso contrário, significaria a inversão do próprio sistema." (STJ, 2013).

Ressalta-se, ademais, a construção de uma interpretação intermediária acerca da admissibilidade da serendipidade. Esse entendimento leva em consideração o momento em que ocorre a descoberta da prova fortuita. Assim, caso a nova evidência surja antes mesmo de ser atingido o objeto probatório que motivou a medida inicial, a sua utilização é considerada válida, ainda que diga respeito a delito diverso. De outro modo, se a descoberta ocorrer apenas após alcançado o objetivo delimitado no mandado, a prova deverá ser considerada ilícita, uma vez que a diligência não pode se prolongar além dos limites previamente fixados pela decisão judicial (Capez, 2021).

Fato é que, independentemente da corrente adotada, é imprescindível observar os parâmetros da necessidade, proporcionalidade e adequação, assegurando a mínima restrição possível aos direitos fundamentais. Soma-se a isso a centralidade do princípio da legalidade, que exige não apenas que a diligência

originária esteja pautada em autorização judicial válida, mas também que o meio empregado respeite integralmente os requisitos legais e os limites expressamente estabelecidos na decisão que a autorizou (Matos, 2022).

Nesse contexto, impõe-se que todas as autoridades envolvidas,magistrados, membros do Ministério Público e autoridades policiais, atuem de forma a maximizar a proteção dos direitos fundamentais e a plena observância do devido processo legal, o que demanda, em especial, decisões judiciais devidamente fundamentadas, mandados com objeto claro e delimitado e observância aos limites impostos na realização das diligências.

4.3 Critérios de validade da prova fortuita em ambiente digital

A partir do que foi delineado no subtópico anterior, não há dúvidas de que a serendipidade constitui fenômeno jurídico reconhecido no processo penal brasileiro, admitindo-se, em determinadas circunstâncias, a validade de provas obtidas de forma fortuita. Parte-se da premissa de que, no curso de diligência regularmente autorizada e estritamente delimitada em seu objeto, pode ocorrer a descoberta de elementos probatórios relevantes, ainda que relacionados a pessoas ou delitos inicialmente não abrangidos pela investigação. Nessas hipóteses, entende-se que a casualidade da obtenção não deve, por si só, servir de obstáculo ao aproveitamento processual da prova.

Por outro lado, é certo que tal entendimento não pode ser aplicado de maneira irrestrita, sob pena de legitimar práticas que desvirtuem a finalidade da diligência e acabem por configurar o fenômeno do *fishing expedition*, repudiado pelo ordenamento jurídico por violar garantias fundamentais e comprometer a admissibilidade das provas dele derivadas.

A problemática assume contornos ainda mais delicados no ambiente digital. Isso porque aparelhos eletrônicos, como smartphones e computadores, concentram um vasto universo informacional, muito superior àquele que se poderia encontrar em buscas tradicionais realizadas em espaços físicos. Conversas mantidas em aplicativos de mensagens, áudios, vídeos, fotografias, dados de geolocalização, registros de navegação e até mesmo arquivos já deletados podem

ser recuperados e acessados, ampliando significativamente os riscos de devassas desproporcionais.

Assim, no contexto de uma realidade cada vez mais permeada pelo mundo digital, medidas investigativas como interceptações telemáticas, quebras de sigilo e buscas em dispositivos eletrônicos tornaram-se recorrentes, mas sua execução prática tem revelado problemas significativos. Como observa Quito (2020), não raro os mandados judiciais autorizadores deixam de delimitar, de forma precisa, o objeto da diligência, autorizando genericamente o acesso a todo o conteúdo de um dispositivo ou a registros em nuvem. Essa amplitude excessiva, somada ao volume e à diversidade das informações armazenadas, pode gerar extrapolações que atingem de forma desproporcional direitos fundamentais como a privacidade (art. 5º, X, CF) e o sigilo das comunicações (art. 5º, XII, CF), ainda que não se constate desvio intencional de finalidade.

Diante desse quadro, mostra-se indispensável fomentar a discussão acerca da fixação de critérios específicos para a aplicação do princípio da serendipidade em ambiente digital. Tais critérios devem ter como ponto de partida a restrição mínima aos direitos fundamentais, observados os parâmetros da razoabilidade e da proporcionalidade, que, como já exposto, desdobram-se em adequação, necessidade e proporcionalidade em sentido estrito. Em qualquer hipótese, não podem ser descurados os direitos à intimidade, à privacidade, à inviolabilidade das comunicações e à inadmissibilidade das provas ilícitas, já analisados ao longo deste trabalho.

Todavia, tais premissas, embora necessárias, não bastam para resolver a controvérsia. Como bem ressaltam Cordeiro, Agosti e Camargo (2024), o debate transcende os exemplos clássicos da doutrina,como a apreensão fortuita de drogas, documentos ou armas durante o cumprimento de mandados de busca e apreensão, pois, nesses casos, dificilmente se questiona a legalidade do achado, desde que não haja desvio de finalidade.

A dificuldade surge quando se trata de dados armazenados em dispositivos eletrônicos, nos quais a amplitude e a natureza sensível das informações exigem interpretação à luz da Constituição. Isso porque o Código de

Processo Penal, datado de 1940, foi concebido em realidade diversa, incapaz de prever a concentração, em um único aparelho, de quase todos os aspectos da vida privada de um indivíduo. Assim, a análise da serendipidade digital não pode ser dissociada do direito fundamental à inviolabilidade da vida privada, do sigilo das comunicações e da proteção de dados pessoais.

Nesse cenário, a prática demonstra que, muitas vezes, as requisições formuladas pelas autoridades de persecução penal autorizam acessos genéricos e ilimitados a dispositivos eletrônicos, sem estabelecer critérios objetivos. Uma forma de conter tais abusos é a delimitação clara do escopo da diligência, especificando quais dados ou aplicativos podem ser acessados e quais estão fora do alcance da medida. Afinal, se dispositivos eletrônicos concentram arquivos de natureza variada como vídeos, áudios, mensagens instantâneas, registros de geolocalização e históricos de navegação, nada justifica, por exemplo, o acesso irrestrito a dados de localização ou de navegação na internet quando o objeto da investigação é restrito à prática de sonegação fiscal, cujo interesse se vincula à localização de notas fiscais fraudulentas (Cordeiro; Agosti; Camargo, 2024).

Outro critério essencial é a limitação temporal, tendo em vista que, se a investigação se refere a fato praticado em período específico, não é admissível autorizar o exame de dados relativos a intervalos de tempo muito mais amplos, que não guardam pertinência com o objeto investigado.

Cumpre ainda mencionar a corrente doutrinária desenvolvida no direito norte-americano, que pode ser refletida e, com as devidas adaptações, servir de inspiração ao processo penal brasileiro. Trata-se da chamada *plain view doctrine* (doutrina da visibilidade imediata),segundo a qual se admite a utilização como prova de objetos encontrados por agentes estatais que atuem sem ou além dos limites do mandado judicial, desde que observadas três condições cumulativas: (i) a evidência deve estar imediatamente visível; (ii) o agente deve ter causa legítima para estar no local de onde visualizou a prova; e (iii) o objeto encontrado, por si só ou em conjunto com outros elementos já conhecidos pelo agente, deve permitir razoável inferência de conexão com a prática criminosa (Mendes, 2021).

Diante disso, embora não haja previsão expressa semelhante em nosso ordenamento, a reflexão comparada evidencia a necessidade de avançar no debate sobre critérios específicos para a admissibilidade do encontro fortuito de provas em ambiente digital. Urge, nesse sentido, a edição de legislação própria que discipline, de modo claro e objetivo, os limites para o acesso a dados digitais e a utilização de informações encontradas de maneira não preordenada.

Até que isso ocorra, mostra-se indispensável que a atuação judicial e investigativa observe critérios já consolidados: definição clara do objeto da investigação, restrição quanto ao tipo de dado a ser acessado, especificação dos aplicativos ou registros abrangidos,delimitação temporal vinculada ao período dos fatos e adaptação dos elementos da *plain view doctrine.*

Em síntese, constata-se que os critérios delineados representam parâmetros indispensáveis para a validade da prova fortuita em ambiente digital. Essas balizas têm a função de garantir que a serendipidade se mantenha fiel à sua natureza, ou seja, ao aproveitamento legítimo de elementos encontrados de forma casual e incidental, sem que a medida investigativa se converta em verdadeira devassa indiscriminada. Tal desvirtuamento, como se viu, caracterizaria típica hipótese de *fishing expedition*. Assim, a distinção entre esses dois institutos será objeto de análise no subtópico seguinte.

4.4 Distinção entre serendipidade e *fishing expedition*

A partir das conceituações já delineadas, constata-se que os institutos da serendipidade e do *fishing expedition* apresentam pontos de contato que, em uma análise superficial, podem sugerir identidade entre eles. Ambos envolvem a descoberta de elementos probatórios não previstos no escopo inicial da investigação, mas partem de premissas substancialmente distintas: enquanto a serendipidade pressupõe o surgimento de achados casuais no curso de uma diligência legítima e previamente delimitada, o *fishing expedition* caracteriza-se pela busca indiscriminada e especulativa, destituída de causa provável e de limites objetivos.

É justamente dessa aparente proximidade que decorre a necessidade de exame atento. A prática forense demonstra que a linha divisória entre os dois

fenômenos pode ser tênue, permitindo que provas obtidas de forma arbitrária sejam, por vezes, apresentadas como se resultassem de um encontro fortuito. Nessas hipóteses, a diligência abusiva se oculta sob o manto da serendipidade, em tentativa de conferir legitimidade ao que, em verdade, representa grave violação a direitos fundamentais.

Nesse cenário, a atuação do Poder Judiciário revela-se imprescindível. Para evitar confusões conceituais e assegurar a integridade do processo penal, a jurisprudência, especialmente do Superior Tribunal de Justiça, tem delineado critérios aptos a diferenciar a serendipidade do *fishing expedition*.

Cumpre ressaltar, entretanto, que tais parâmetros foram desenvolvidos, de modo mais consistente, no exame de diligências tradicionais, como buscas pessoais, buscas e apreensões domiciliares e interceptações telefônicas. No campo digital, por outro lado, as decisões ainda são incipientes, razão pela qual este subtópico se propõe a revisitar os critérios já consolidados em contextos análogos, adaptando-os às peculiaridades das provas eletrônicas e aos riscos ampliados que elas apresentam.

De início, merece destaque a decisão proferida pelo Superior Tribunal de Justiça no HC n. 663.055/MT (Info 731), de relatoria do Ministro Rogério Schietti Cruz, que reconheceu a ilicitude de provas colhidas em decorrência de desvio de finalidade. Naquele caso, entendeu-se que a atuação policial ultrapassou os limites autorizados judicialmente, o que descaracterizou eventual serendipidade e configurou pescaria probatória. Consta do julgado:

> **É ilícita a prova colhida em caso de desvio de finalidade após o ingresso em domicílio**, seja no cumprimento de mandado de prisão ou de busca e apreensão expedido pelo Poder Judiciário, seja na hipótese de ingresso sem prévia autorização judicial, como ocorre em situação de flagrante delito. **O agente responsável pela diligência deve sempre se ater aos limites do escopo - vinculado à justa causa - para o qual excepcionalmente se restringiu o direito fundamental à intimidade, ressalvada a possibilidade de encontro fortuito de provas(STJ,2022)**

Do referido precedente extrai-se a relevância da delimitação precisa do objeto da diligência e da observância rigorosa ao escopo fixado judicialmente. Isso

porque, sendo medidas que implicam restrição a direitos fundamentais, somente se legitimam pela presença de justa causa e devem ser executadas dentro dos exatos limites da autorização concedida. Caso contrário, as provas obtidas serão ilícitas, seja pela configuração de *fishing expedition*, seja pela violação indevida a direitos e garantias constitucionais do investigado.

Ainda nesse contexto de necessária vinculação ao objeto previamente definido, decisão da Sexta Turma do STJ delimita os contornos dos dois institutos e analisa seu embate dentro de uma mesma circunstância.Vejamos:

> AGRAVO REGIMENTAL NO AGRAVO EM RECURSO ESPECIAL. PROCESSO PENAL. MOEDA FALSA. NULIDADE. INVASÃO DE DOMICÍLIO. AUSÊNCIA DE FUNDADAS RAZÕES PARA O INGRESSO. CUMPRIMENTO DE MANDADO DE PRISÃO. DEVASSA DOMICILIAR. ILEGALIDADE. AGRAVO REGIMENTAL DESPROVIDO. [...]**Admitir a entrada na residência especificamente para efetuar uma prisão não significa conceder um salvo-conduto para que todo o seu interior seja vasculhado indistintamente, em verdadeira pescaria probatória (fishing expedition), sob pena de nulidade das provas colhidas por desvio de finalidade"**(RHC n. 165.982/PR, relator Ministro Rogerio Schietti Cruz, Sexta Turma, julgado em 20/9/2022, DJe de 26/9/2022, grifei). 2. No caso em tela, os agentes policiais alegaram que realizaram a devassa após tentativa de dar cumprimento a mandado de prisão temporária e haver dúvidas quanto à identidade do agente. 4. **Não se pode falar em encontro fortuito de provas, porquanto bem delineado na denúncia que as cédulas falsas foram localizadas dentro do guarda-roupas do acusado, circunstância que extrapola o escopo do cumprimento de mandado de prisão temporária, mormente considerada a necessidade de devassa de vários compartimentos em habitação coletiva, com invasão na esfera de intimidade de diversas outras pessoas**. 5. Agravo regimental desprovido (grifo nosso)(Stj, 2023)

Do precedente extraem-se duas conclusões centrais. A primeira é que a autorização de ingresso em domicílio para cumprimento de mandado de prisão não se confunde com uma licença para vasculhar indistintamente todo o interior da residência.De forma análoga, no âmbito digital, a autorização judicial para acessar determinados dados não pode ser interpretada como permissão irrestrita para explorar a integralidade do conteúdo de um dispositivo eletrônico. Se tal prática já encontra vedação nas diligências físicas, sua reprovação deve ser ainda mais enfática no campo tecnológico, considerando a amplitude e a elevada sensibilidade das informações ali armazenadas.

O segundo aspecto relevante é a recusa em reconhecer a aplicação da serendipidade quando os elementos probatórios somente são obtidos em razão do extrapolamento do escopo autorizado. Esse critério revela-se crucial em qualquer análise destinada a verificar se a prova foi, de fato, fruto de um achado fortuito ou se decorreu de uma verdadeira pescaria probatória. Afinal, uma vez ultrapassados os limites fixados na decisão judicial, não há que se falar em encontro fortuito, mas em prática manifestamente ilegal.

Em complemento, deve-se ressaltar que, nos casos em que o objeto da diligência já tenha sido alcançado e ainda assim os agentes prosseguem com a busca, a continuidade da medida não se caracteriza como descoberta fortuita, mas como pescaria probatória, tendo em vista que o direcionamento deliberado da investigação para fatos não contemplados pela decisão judicial revela manifesto desvio de finalidade

Esse entendimento foi reforçado em decisão recente no RHC n. 194.639/SC (2024/0072902-9), em que o STJ tratou do tema no contexto digital. Na oportunidade, a Corte distinguiu de forma expressa o encontro fortuito de provas da pescaria probatória, nos seguintes termos:

> “O Superior Tribunal de Justiça (STJ) tem jurisprudência consolidada sobre a validade das provas obtidas por interceptação telefônica e a prática conhecida como " fishing expedition" (pescaria probatória) que difere do "encontro fortuito de prova". Esta Corte diferencia a prática da pescaria probatória do fenômeno do "encontro fortuito de provas" (serendipidade), que ocorre quando, durante uma investigação legalmente autorizada, surgem provas inesperadas relacionadas a crimes não inicialmente investigados. A serendipidade é aceita, desde que respeite os limites legais e constitucionais”

No caso em exame, a defesa alegou a nulidade das provas por suposto acesso amplo e indiscriminado a registros digitais armazenados em serviços de nuvem, vinculados a contas dos investigados em plataformas como Google, Instagram, Facebook e Apple, bem como a dados extraídos de seus dispositivos eletrônicos .

O Superior Tribunal de Justiça, entretanto, assentou que são válidas as provas encontradas casualmente pelos agentes da persecução penal, relativas a infração penal até então desconhecida, reveladas por ocasião do cumprimento de

medidas de investigação de outro delito regularmente autorizadas, ainda que inexista conexão ou continência com o crime supervenientemente identificado, desde que não haja desvio de finalidade na execução das diligências que originaram tais elementos probatórios.

Diante de todo o exposto, percebe-se que a distinção entre serendipidade e *fishing expedition* repousa, essencialmente, na existência ou não de extrapolação do escopo definido pela decisão judicial. Para tanto, deve-se avaliar, em cada caso concreto, se: (i) a diligência foi previamente autorizada pela autoridade judicial competente; e (ii) se a prova surgiu dentro dos limites fixados ou decorreu de desvio de finalidade. A resposta a essas indagações permite classificar a prova como legítima e lícita ou, ao contrário, como fruto de prática abusiva e inconstitucional.

É justamente nesse contexto que emerge a necessidade de fundamentação específica nos mandados de autorização das diligências, sejam elas de acesso a dados armazenados, a dados em fluxo, à busca e apreensão de aparelhos eletrônicos ou ao infiltramento de agentes em aplicativos de mensagens. Afinal, é a decisão judicial que delimita o que efetivamente pode ser investigado e o que deve permanecer protegido.

Assim, a expedição de ordens genéricas gera grave insegurança jurídica, pois inviabiliza a distinção entre o que efetivamente se encontra dentro ou fora do escopo autorizado, conduzindo à indevida ampliação da medida e à falsa impressão de que todo e qualquer dado estaria abrangido pela decisão judicial. Tal generalidade compromete a possibilidade de controle sobre desvios de finalidade e favorece práticas investigativas abusivas. Diante disso, impõe-se examinar, no subtópico seguinte, a problemática dos mandados judiciais genéricos e os limites que devem orientar a atuação estatal na persecução penal.

4.5 Mandados judiciais genéricos e os limites da atuação estatal

Com a expansão das investigações em meio digital, tornou-se frequente a apreensão e o exame de vastos volumes de dados pessoais. Nesse cenário, evidencia-se um problema estrutural: a ausência de regulamentação legal específica. Embora os regimes da interceptação telefônica, das buscas e

apreensões e as diretrizes do Marco Civil da Internet ofereçam balizas relevantes, não são suficientes para abranger as peculiaridades técnico-operativas do universo informacional, tampouco para suprir integralmente as lacunas existentes.

Projetos legislativos têm buscado reduzir esse déficit normativo, a exemplo do PL n.º 4.939/2020, que estabelece princípios de Direito da Tecnologia da Informação e critérios para obtenção e admissibilidade de provas digitais. Entretanto, enquanto não sobrevier marco legal próprio, cabe ao processo penal adaptar-se às novas realidades tecnológicas, reinterpretando institutos tradicionais à luz da Constituição e recorrendo a critérios doutrinários e jurisprudenciais que, ainda que de forma provisória, preencham as lacunas normativas.

Nesse quadro de normatividade insuficiente, surge um segundo ponto crítico: a recorrência de mandados judiciais genéricos. Observa-se a expedição de ordens de busca, quebras de sigilo, acessos a dados e requisições a provedores com formulações vagas, que, na prática, franqueiam o exame irrestrito do conteúdo integral de dispositivos ou de extensas bases de registros, sem definição clara do que deve ser efetivamente coletado. Como assinalam Barbosa e Russi, a generalidade decisória desloca o foco da prova necessária para uma procura difusa por “qualquer evidência”, aproximando a medida da indevida pescaria probatória (Barbosa; Russi, 2024).

Sob perspectiva metodológica, emergem indagações inevitáveis: como identificar desvio de finalidade quando a própria finalidade não foi previamente delimitada? Como diferenciar o que foi genuinamente encontrado dentro do escopo legítimo do que decorreu de vasculhamento incompatível com a autorização? Tais dúvidas decorrem, quase sempre, da ausência de delimitação nas ordens que disciplinam a colheita de evidências digitais, circunstância que favorece a ocorrência de *fishing expedition*, diante da amplitude das autorizações, da falta de contornos específicos e da ausência de causa provável idônea para a extensão dos dados pretendida (Silva; Silva; Rosa, 2019).

Em sentido oposto ao que frequentemente se observa na prática forense, a legislação e a doutrina impõem fundamentação idônea e especificidade nas autorizações judiciais. Para Rosa, toda medida probatória sujeita à reserva de jurisdição deve, de antemão, responder a quem, quando, como, onde, por que e

para quê, com motivação capaz de demonstrar a necessidade, a adequação e a proporcionalidade da medida, sob pena de nulidade, nos termos do art. 315, § 2º, do Código de Processo Penal (Rosa, 2021). Nessa mesma linha, Pitombo rechaça o “mandado incerto, vago ou genérico”, exigindo que a decisão explicite local, motivo, finalidade e autoridade expedidora (Pitombo, 2005).

Nessa linha, Aury Lopes sintetiza a razão de ser da especialidade na premissa de que mandados genéricos,inclusive varreduras em áreas inteiras,subvertem o regime de exceção das medidas invasivas e afrontam o art. 243, II, do CPP, que exige indicação clara do local, dos motivos e dos fins da diligência; daí a ilicitude de “cartas brancas” que autorizem buscas sem foco, como reconhecido pelo STJ ao invalidar, em habeas corpus coletivo, “buscas coletivas” em comunidades por ausência de individualização e violação a regras constitucionais e processuais (Lopes Jr., 2025).

No plano digital, a necessidade de delimitação do objeto é ainda mais evidente, tendo em vista que a vastidão e a interdependência dos registros, a frequência com que metadados se acoplam a conteúdos e a própria arquitetura de armazenamento tornam real o risco de devassa informacional quando o título judicial não fixa contornos claros. Por isso, não basta autorizar, em termos genéricos, “o acesso ao smartphone” ou “ao computador”. É imprescindível indicar, com precisão, o conteúdo pertinente à persecução,aplicativos, conversas, caixas postais ou repositórios e a moldura temporal da análise.

Em termos práticos, se a medida incide sobre WhatsApp, Telegram ou Facebook, a decisão, tanto quanto possível, deve apontar conversas ou grupos, intervalo de datas e, quando cabível, horários, prevenindo-se a devassa dissociada do objeto investigado (Matos, 2022).

Idêntica cautela se impõe nas interceptações telefônicas e telemáticas e nas quebras de sigilo de dados. Isso porque, autorizações genéricas nesses domínios favorecem o mascaramento de incursões exploratórias sob a roupagem de “achado fortuito”, dada a amplitude de dados e metadados potencialmente alcançáveis. O resultado é a violação simultânea de direitos fundamentais, tais como privacidade, intimidade,presunção de inocência e, no contexto de hiperconcentração

informacional, do próprio privilégio contra a autoincriminação, em afronta direta aos parâmetros da necessidade, adequação e proporcionalidade.

Diante disso, a jurisprudência recente tem reafirmado a centralidade da especificidade na prova digital. O Tribunal de Justiça de Goiás, ao denegar habeas corpus, manteve decisões que autorizaram a quebra de sigilo de dados de celulares apreendidos por se encontrarem “dentro dos parâmetros adequados, com delimitação precisa do objeto de acesso**”**, ressaltando que, mesmo diante de justa causa e utilidade, a validade da medida depende da moldura traçada pelo magistrado (Brasil,2024).

A controvérsia sobre autorizações amplas também se projeta nas chamadas buscas reversas perante provedores. No Mandado de Segurança n. 2299215-62.2022.8.26.0000, o Tribunal de Justiça de São Paulo examinou ordem que determinava ao Google o fornecimento de dados cadastrais de todos os usuários que, em curto lapso temporal, transitaram em raio de 100 metros do local de um latrocínio. As impetrantes alegaram a natureza genérica e invasiva da medida, por ausência de individualização e variabilidade técnica da geolocalização.

O Tribunal, contudo, reputou atendidos os requisitos do art. 22 do Marco Civil(indícios fundados, justificativa motivada e delimitação temporal) e destacou o recorte espaço-temporal e o segredo de justiça, concluindo pela proporcionalidade e adequação do provimento ao esclarecimento da autoria (Brasil,2024).

No Supremo Tribunal Federal, o debate ganhou relevo com a recente tese do Ministro Alexandre de Moraes, no Tema 1.148 da repercussão geral (RE 130125), acerca da constitucionalidade da requisição judicial de registros de conexão e de acesso a aplicações, inclusive em “buscas reversas por palavra-chave”, com fundamento no art. 22 do Marco Civil da Internet, desde que observados indícios do ilícito, justificativa de utilidade, delimitação temporal e proporcionalidade.

De forma crítica, o Ministro André Mendonça advertiu para os riscos de autorizações voltadas a universos indeterminados de pessoas, sem qualquer elemento prévio de suspeita, ressaltando que tais práticas afrontam diretamente os princípios constitucionais do devido processo legal e da intimidade.

Em seu voto, propôs critérios mais rigorosos, como a especificação precisa do tipo de dado solicitado, a análise do grau de exposição decorrente do compartilhamento, a correlação clara entre investigados e objeto da investigação, a demonstração da imprescindibilidade, a base em suspeitas fundamentadas e regras de custódia e descarte das informações inservíveis, com observância dos arts. 7º, 10, §§ 1º e 2º, e 22 do Marco Civil. Argumentou, ainda, que redações vagas podem abrir espaço a medidas excessivamente abrangentes. Tais parâmetros harmonizam-se com as premissas defendidas neste trabalho, reforçando o combate às autorizações genéricas e à prática da *fishing expedition.*

Na data da presente redação, o julgamento definitivo permanece pendente em razão do pedido de vista do Ministro Gilmar Mendes, o que evidencia a atualidade e a complexidade do tema. Persistem, portanto, controvérsias quanto à possibilidade de investigações envolvendo indivíduos indeterminados, ainda que delimitados espaço-temporalmente, e a busca por equilibrar a efetiva proteção dos bens jurídicos com a tutela dos direitos fundamentais.

Por fim, cabe destacar um efeito prático frequentemente negligenciado.Mandados genéricos não apenas fragilizam direitos fundamentais e tornam nebulosa a distinção entre serendipidade e *fishing expedition*, mas também comprometem a própria eficácia da investigação. Nulidades processuais por excesso de escopo ou por fundamentação padronizada podem levar à inadmissão de provas relevantes, atrasar a persecução penal e frustrar a finalidade legítima da jurisdição penal.

Diante disso, compreende-se que a fundamentação adequada e a delimitação objetiva do objeto da medida não constituem meras formalidades, mas verdadeiros instrumentos de combate a abusos. O Poder Judiciário ocupa posição central nesse cenário, pois é dele que emanam as autorizações que legitimam a restrição de direitos fundamentais. Daí a necessidade de que essas decisões estejam adaptadas à realidade tecnológica contemporânea, estabelecendo com precisão a finalidade e a abrangência das diligências, de modo a restringir ao mínimo os direitos fundamentais e, ao mesmo tempo, permitir que eventuais provas fortuitas sejam admitidas sem que se confunda sua validade com práticas ilegítimas de devassa indiscriminada.

5 CONSIDERAÇÕES FINAIS

Em face do protagonismo exponencial das redes digitais no cotidiano dos indivíduos e da consequente ampliação dos riscos de deturpação das diligências investigativas e de violação às garantias constitucionais, mostra-se inadiável a construção de parâmetros seguros para a admissibilidade da prova digital no processo penal. Essa necessidade constituiu o problema de pesquisa que norteou o presente trabalho, voltado ao exame das condições em que é possível admitir a prova digital, especialmente quando obtida de forma fortuita, considerando-se as limitações impostas pelos direitos e garantias fundamentais, bem como a vedação às práticas de *fishing expedition*.

A análise realizada permitiu demonstrar que os objetivos propostos foram alcançados, à medida que foram sistematizados critérios jurídicos capazes de orientar a atuação judicial e investigativa no tocante à admissibilidade da prova digital, sobretudo enquanto não sobrevier legislação específica. O primeiro critério consiste na observância da cadeia de custódia, tendo em vista que, dada a natureza volátil e a elevada manipulabilidade das provas digitais, a rastreabilidade e a autenticidade devem ser rigorosamente documentadas, de forma a evitar que elementos adulterados comprometam a higidez da persecução penal.

O segundo critério corresponde à restrição mínima aos direitos fundamentais, especialmente àqueles mais vulneráveis no meio digital, como a intimidade, a privacidade e o sigilo das comunicações, notoriamente expostos diante da vastidão de dados e da facilidade de coleta em massa. A observância da proibição das provas ilícitas e do direito à não autoincriminação integra, igualmente, esse parâmetro, reforçando a necessidade de compatibilizar a persecução penal com a tutela dos direitos fundamentais.

Em continuidade, impõe-se destacar como critério essencial a exigência de autorização judicial prévia para as diligências em ambiente digital. As diversas formas de obtenção de provas, tais como acesso a dados armazenados, análise de comunicações em fluxo, requisição de informações a provedores, infiltrações de agentes virtuais e buscas em dispositivos eletrônicos somente podem ser

validamente realizadas mediante ordem judicial. Tal requisito constitui pressuposto elementar de legalidade, na medida em que a ausência de autorização compromete de forma absoluta a higidez do material colhido, tornando inviável a aferição dos demais parâmetros de admissibilidade.

Associada a essa exigência encontra-se a fundamentação e a especificidade da decisão judicial. Não basta a mera autorização genérica de acesso a dispositivos ou bases de dados, sendo indispensável que o magistrado delimite, com clareza, os elementos que podem ser alcançados, os aplicativos ou repositórios abrangidos e o período temporal pertinente. Esse detalhamento é o que confere legitimidade à medida e garante que a investigação se desenvolva dentro de limites objetivos, evitando interpretações ampliativas que conduzam a devassas informacionais desproporcionais.

Assim, verifica-se que a observância desses parâmetros é decisiva para diferenciar a serendipidade, caracterizada pelo encontro fortuito de provas durante a execução de uma diligência válida e delimitada, da *fishing expedition*, que se traduz na busca indiscriminada, especulativa e sem justa causa. No ambiente digital, em que a linha entre esses fenômenos é particularmente tênue, apenas as provas surgidas de forma fortuita, no estrito cumprimento do escopo definido pelo mandado, podem ser admitidas. Já aquelas obtidas em desvio de finalidade ou mediante buscas genéricas devem ser reputadas ilícitas, por configurarem prática arbitrária incompatível com o ordenamento jurídico brasileiro.

Ainda nesse contexto, integram o rol de critérios a existência de justa causa e a vedação à continuidade das buscas após alcançado o objetivo inicialmente definido. A vinculação da diligência à sua finalidade específica constitui exigência inafastável, diretamente relacionada à fundamentação da autorização judicial e à preservação da legalidade do ato investigativo.

A partir desses parâmetros, conclui-se que a admissibilidade das provas digitais fortuitas é possível, mas está condicionada ao respeito estrito aos limites constitucionais e processuais.

Não obstante os avanços doutrinários e jurisprudenciais, resta evidente a necessidade de atualização legislativa para contemplar as peculiaridades do

ambiente digital. Projetos como o PL nº 4.939/2020, que estabelece diretrizes para a obtenção e admissibilidade de provas digitais, criminaliza condutas informáticas e disciplina a redação de mandados judiciais, e o PL nº 4.291/2020, que altera o Código de Processo Penal para tratar da custódia de elementos digitais de prova, representam passos fundamentais na superação das lacunas normativas. A urgência dessa atualização é ainda mais notória em modalidades altamente invasivas, como o acesso remoto e oculto por hacking estatal e o uso de malwares (subtópico 2.2.2), que não podem ser reguladas por analogia a institutos tradicionais, sob pena de grave insegurança jurídica.

Enquanto não se concretiza a aprovação de tais legislações, cabe ao Poder Judiciário, ao Ministério Público e às autoridades policiais atuarem de maneira coordenada e responsável, assegurando que as diligências sejam conduzidas dentro dos parâmetros constitucionais. Essa postura é essencial para prevenir abusos, evitar nulidades processuais e garantir que a persecução penal de delitos cometidos no ambiente cibernético não seja inviabilizada por vícios de legalidade ou de legitimidade.

Diante de todo o exposto, conclui-se que o presente trabalho contribui não apenas para o debate acadêmico, mas também para a prática forense, ao propor critérios objetivos que orientam a admissibilidade da prova digital e fornecem subsídios relevantes para a elaboração de futura legislação específica. Ao reafirmar que a eficácia da persecução penal deve avançar em sintonia com a preservação dos direitos fundamentais, este estudo reforça o compromisso do processo penal com os valores do Estado Democrático de Direito, demonstrando que o avanço tecnológico exige, como contrapartida, uma evolução normativa e hermenêutica capaz de assegurar a legitimidade da jurisdição penal.

REFERÊNCIAS

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27037:2012 – Tecnologia da informação – Técnicas de segurança – Diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Rio de Janeiro, 2013. Disponível em: https://www.abntcatalogo.com.br/norma.aspx?ID=307273. Acesso em: 20 mai 2025.

ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. Vigilância sobre as comunicações no Brasil: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais. São Paulo: InternetLab, 2017. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2017/05/Vigilancia_sobre_as_comunicacoes_no_Brasil_2017_InternetLab.pdf. Acesso em: 2 jul. 2025.

ALBECHE, Thiago Solon Gonçalves. Prova digital, investigação cinética e o princípio da parametrização do novo meio de obtenção de prova. *Meu Site Jurídico*, 10 out. 2023. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2023/10/10/prova-digital-investigacao-cinetica-e-o-principio-da-parametrizacao-do-novo-meio-de-obtencao-de-prova/. Acesso em: 28 jul. 2025.

ALEXY, Robert. Teoria da argumentação jurídica. Trad. Zilda Hutchinson Shild Silva. São Paulo: Landy, 2001.

ASSUMPÇÃO, A. O uso do espelhamento via WhatsApp Web como prova no processo penal. Boletim IBCCRIM, São Paulo, v. 32, n. 380, p. 22-24, 2024. DOI: 10.5281/zenodo.11175866. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1079. Acesso em: 14 abr. 2025.

AVENA, Norberto. Processo penal. 15. ed. Rio de Janeiro: Método, 2023. E-book. ISBN 9786559647774. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786559647774/. Acesso em: 11 ago. 2025.

BADARÓ, Gustavo. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. Boletim IBCCRIM, São Paulo, ano 29, n. 343, p. 7-9, jun. 2021. Disponível em: https://www.ibccrim.org.br/publicacoes/exibir/747. Acesso em: 7 ago. 2025.

BARBOSA ARAUJO, Karen Tayne; MARIOZI RUSSI, Leonardo. A prática abusiva do “fishing expedition” no mandado de busca e apreensão. Revista Científica Eletrônica de Ciências Aplicadas da FAIT, v. 9, n. 2, out. 2024.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 17 mar. 2025.

BRASIL. Congresso Nacional. Projeto de Lei nº 4.291, de 2020. Altera o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para dispor sobre a cadeia de custódia dos elementos digitais de prova. Brasília, DF: Câmara dos Deputados, 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1954521&filename=Avulso%20PL%204291/2020. Acesso em: 03 jun.2025

BRASIL. Congresso Nacional. Projeto de Lei nº 4.939, de 2020. Estabelece princípios e diretrizes para a aplicabilidade do Direito da Tecnologia da Informação, bem como normas sobre obtenção e admissibilidade de provas digitais. Brasília, DF: Congresso Nacional, 2020. Disponível em: https://www25.senado.leg.br/web/ativi21.dade/materias/-/materia/144375. Acesso em: 05 jun.2025

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Diário Oficial da União: seção 1, Brasília, DF, 31 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 07 jun.2025

BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. Diário Oficial da União: seção 1, Brasília, DF, 13 out. 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 10 jun.2025

BRASIL. Lei nº 9.296, de 24 de julho de 1996. Dispõe sobre a interceptação de comunicações telefônicas. Diário Oficial da União: seção 1, Brasília, DF, 25 jul. 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 12 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 da prova, infrações penais correlatas e o procedimento criminal. Diário Oficial da União: seção 1, Brasília, DF, ano 150, n. 148, 5 ago. 2013. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 18 mai.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: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 14 mai.2025

BRASIL. Lei nº 13.105, de 16 de março de 2015. Código de Processo Civil. Diário Oficial da União: seção 1, Brasília, DF, 17 mar. 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em:18 mai.2025

BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade n. 6.298*. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5840274. Acesso em: 01 jun.2025

BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade n. 6.299*. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5840373. Acesso em: 01 jun.2025

BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade n. 6.300*. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5840552. Acesso em: 01 jun.2025

BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade n. 6.305*. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5844852. Acesso em: 01 jun.2025

BRASIL. Supremo Tribunal Federal. Habeas Corpus nº 91.867/PA. Relator: Min. Gilmar Mendes. Brasília, DF, 24 abr. 2012. Disponível em:https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=2792328.. Acesso em: 16 jun.2025

BRASIL. Supremo Tribunal Federal. Habeas Corpus nº 129.678/SP. Relator originário: Min. Marco Aurélio. Redator para o acórdão: Min. Alexandre de Moraes. 1ª Turma. Brasília, DF, 13 jun. 2017. Informativo nº 869. Disponível em:https://www.stf.jus.br/arquivo/informativo/documento/informativo869.htm. Acesso em: 10 jun.2025

BRASIL. Supremo Tribunal Federal. Mandado de Segurança nº 21.729. Relator: Min. Néri da Silveira. Voto: Min. Sepúlveda Pertence. Brasília, DF, 5 out. 1995. Diário da Justiça da União, Brasília, DF, 19 out. 2001.

BRASIL. Supremo Tribunal Federal. Tema 1.148 da Repercussão Geral. Requisição judicial de registros de conexão e de acesso a aplicações de internet. Relator: Min. Alexandre de Moraes. Julgamento suspenso por pedido de vista. Brasília, DF. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6059876. Acesso em: 24 ago.2025

BRASIL. Superior Tribunal de Justiça. Habeas Corpus nº 187.189/SP. Relator: Min. Og Fernandes. 6ª Turma. Brasília, DF, 13 ago. 2013. Diário da Justiça Eletrônico, 23 ago. 2013. Disponível em:https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ITA?seq=1246168&tipo=0&nreg=201001857091&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20130823&formato=PDF&salvar=false. Acesso em: 24 mai.2025

BRASIL. Superior Tribunal de Justiça. Recurso em Habeas Corpus nº 51.531/RO. Relator: Min. Nefi Cordeiro. Brasília, DF, 9 maio 2016. Diário da Justiça Eletrônico, 9 maio 2016. Disponível em:https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ATC?seq=55017400&tipo=5&nreg=201402323677&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20160509&formato=PDF&salvar=false. Acesso em: 17 mai.2025

BRASIL. Superior Tribunal de Justiça. Recurso em Habeas Corpus nº 143.169/RJ. Relator: Min. Ribeiro Dantas. 6ª Turma. Brasília, DF, 7 fev. 2023. Revista do STJ, Brasília, DF, 2023. Disponível em:

https://www.stj.jus.br/revistaeletronica/ita.asp?registro=202201169744. Acesso em: 2 ago.2025

BRASIL. Superior Tribunal de Justiça. Agravo Regimental no Recurso em Habeas Corpus nº 184.003/SP. Relatora: Min. Daniela Teixeira. 6ª Turma. Brasília, DF, 10 dez. 2024. Disponível em: https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/d6055de68dad5a21a33d640118198c98. Acesso em: 6 ago. 2025.

BRASIL. Superior Tribunal de Justiça. REsp n. 1.782.386/RJ. Relator: Ministro Joel Ilan Paciornik. Quinta Turma. Brasília, DF, 15 dez. 2020. DJe 18 dez. 2020. Disponível em: https://processo.stj.jus.br/processo/julgamento/eletronico/documento/?documento_tipo=integra&documento_sequencial=119581748&registro_numero=201803152161&publicacao_data=20201218. Acesso em: 9 ago. 2025

BRASIL. Superior Tribunal de Justiça. *Habeas Corpus* n. 663.055/MT. Relator: Ministro Rogerio Schietti Cruz. 6ª Turma. Brasília, DF, julgado em 22 mar. 2022. *Diário da Justiça Eletrônico*, 31 mar. 2022. Disponível em: https://processo.stj.jus.br/processo/julgamento/eletronico/documento/?documento_tipo=integra&documento_sequencial=148829275&registro_numero=202101288508&publicacao_data=20220331. Acesso em: 7 ago. 2025.

BRASIL. Superior Tribunal de Justiça. *Recurso em Habeas Corpus* n. 194.639/SP. Relator: Ministro Messod Azulay Neto. 6ª Turma. Brasília, DF, julgado em 14 abr. 2025. *Diário da Justiça Eletrônico*, 22 abr. 2025. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/4462781732/inteiro-teor-4462781762. Acesso em: 5 ago. 2025.

BRASIL. Tribunal de Justiça de Goiás. *Habeas Corpus* n. 5365814-02.2024.8.09.0107. Relator: Desembargador Adegmar José Ferreira. 4ª Câmara Criminal. Goiânia, GO, julgado em 6 jun. 2024. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-go/2543109232. Acesso em: 30 ago. 2025.

CAMBI, Eduardo; PITTA, Rafael Gomiero. Discovery no processo civil norte-americano e efetividade da justiça brasileira. *Revista dos Tribunais*, São Paulo, v. 40, n. 245, jul. 2015.

CAPEZ, Fernando. Curso de processo penal. 31. ed. Rio de Janeiro: Saraiva Jur, 2024. E-book. ISBN 9788553620821. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788553620821/. Acesso em: 23 jul. 2025.

CAPEZ, Fernando. Serendipidade, o encontro fortuito de prova. *Consultor Jurídico,* São Paulo, 20 maio 2021. Disponível em: https://www.conjur.com.br/2021-mai-20/serendipidade-encontro-fortuito-prova. Acesso em: 19 ago. 2025.

CASTRO, Matheus Felipe de. Um celular na cena do crime: o STF e a proteção dos dados estáticos. *Consultor Jurídico*, São Paulo, 20 set. 2024. Disponível em:

https://www.conjur.com.br/2024-set-20/um-celular-na-cena-do-crime-o-stf-e-a-protecao-dos-dados-estaticos/. Acesso em: 24 jul. 2025.

CAVALCANTE, Márcio André Lopes. A corrupção de parte dos arquivos compromete a integralidade da prova, inviabilizando sua utilização. Buscador Dizer o Direito, Manaus, 6 ago. 2025. Disponível em: https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/d6055de68dad5a21a33d640118198c98. Acesso em: 6 ago. 2025.

CAVALCANTE, Márcio André Lopes. A determinação judicial para identificação dos usuários que operaram em determinada área geográfica, suficientemente fundamentada, não ofende a proteção à privacidade e à intimidade. Buscador Dizer o Direito, Manaus, 10 ago. 2025. Disponível em: https://buscadordizerodireito.com.br/jurisprudencia/detalhes/8fc4bc380e6185d2f37a64f0c8f34a93. Acesso em: 10 ago. 2025.

CAVALCANTE, Márcio André Lopes. A falta de procedimentos para garantir a idoneidade e integridade dos dados extraídos de um celular apreendido resulta na quebra da cadeia de custódia e na inadmissibilidade da prova digital. Buscador Dizer o Direito, Manaus, 7 ago. 2025. Disponível em: https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/646e058fac455de8d1e52c4c49baac06. Acesso em: 7 ago. 2025.

CAVALCANTE, Márcio André Lopes. A autorização judicial para que a polícia acompanhe as conversas dos suspeitos mediante o espelhamento via WhatsApp Web caracteriza-se como um meio de obtenção de prova equivalente à infiltração de agentes, sendo, portanto, extraordinário, mas válido. Buscador Dizer o Direito, Manaus, 10 ago. 2025. Disponível em: https://buscadordizerodireito.com.br/jurisprudencia/detalhes/eafd9b2037cb218fafd3aa05535c123e. Acesso em: 10 ago. 2025.

CAVALCANTE, Márcio André Lopes. É possível a utilização de ações encobertas, controladas virtuais ou de agentes infiltrados no plano cibernético, inclusive via espelhamento do WhatsApp Web, desde que o uso da ação controlada na investigação criminal esteja amparada por autorização judicial. Buscador Dizer o Direito, Manaus, 10 ago. 2025. Disponível em: https://buscadordizerodireito.com.br/jurisprudencia/detalhes/b31f0c758bb498b5d56b5fea80f313a7. Acesso em: 10 ago. 2025.

CAVALCANTE, Márcio André Lopes. São inadmissíveis as provas digitais sem registro documental acerca dos procedimentos adotados pela polícia para a preservação da integridade, autenticidade e confiabilidade dos elementos informáticos. Buscador Dizer o Direito, Manaus, 7 ago. 2025. Disponível em: https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/194585b5215aea447389c5fefca09c61. Acesso em: 7 ago. 2025.

CONVENÇÃO AMERICANA DE DIREITOS HUMANOS. *Pacto de San José da Costa Rica* (1969). San José, 22 nov. 1969. Ratificada pelo Brasil em 25 set. 1992. Disponível em: https://www.pge.sp.gov.br/centrodeestudos/bibliotecavirtual/instrumentos/sanjose.htm. Acesso em: 18 ago. 2025.

CORDEIRO, Pedro Ivo Rodrigues Velloso; AGOSTI, Francisco Felippe Lebrão; CAMARGO, Pedro Luís de Almeida. Repensando o encontro fortuito de provas na era digital. *Boletim IBCCRIM,* São Paulo, v. 32, n. 384, p. 21-26, 2024. DOI: https://doi.org/10.5281/zenodo.13834573. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1658. Acesso em: 1 ago.2025

FURLANETO, Mário Neto; SANTOS, José. Apontamentos sobre a cadeia de custódia da prova digital no Brasil. *Revista Em Tempo*, Marília, 2020, p. 8–9. Disponível em: https://revista.univem.edu.br/emtempo/article/view/3130/940. Acesso em: 3 abr. 2021.

GRECO, Luís; GLEIZER, Orlandino. A infiltração online no processo penal: notícia sobre a experiência alemã. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 5, n. 3, p. 1483–1518, set./dez. 2019. DOI: https://doi.org/10.22197/rbdpp.v5i3.278

JANGUTTA, Kátia Maria Amaral. Acesso a dados armazenados em dispositivos móveis para fins de investigação: a licitude da prova e a atuação do Poder Judiciário. In: ANTONIALLI, Dennys; FRAGOSO, Nathalie (org.). *Direitos fundamentais e processo penal na era digital: doutrina e prática em debate*. São Paulo: InternetLab, v. 2, 2019. p. 24–40. Disponível em: .https://www.internetlab.org.br/wp-content/uploads/2019/08/InternetLabCongressoII_dupla.pdf. Acesso em: 17 jul.2025

LIMA, Renato Brasileiro de. *Manual de processo penal: volume único*. 8. ed. rev., ampl. e atual. Salvador: Ed. JusPodivm, 2022.

LOPES JR., Aury. *Direito Processual Penal*. 22. ed. Rio de Janeiro: SRV, 2025. E-book. p. 399. ISBN 9788553625673. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788553625673/. Acesso em: 23 jul. 2025.

MATOS, Daniel Freitas. *O uso de provas digitais e a vedação ao fishing expedition no processo penal brasileiro*. Monografia (Bacharelado em Direito) – Universidade Federal de Minas Gerais, Faculdade de Direito, Belo Horizonte, 2022.

MENDES, Carlos Hélder C. Furtado. *Malware do Estado e processo penal: a proteção de dados informáticos face à infiltração por software na investigação criminal*. 2018. Dissertação (Mestrado) – PUCRS, Porto Alegre, 2018.

MENDES, Carlos Hélder C. Furtado. *Tecnoinvestigação Criminal: entre a proteção de dados e a infiltração por software*. 1. ed. Salvador: Editora Juspodivm, 2020.

MENDES, Paulo de Sousa. A privacidade digital posta à prova no processo penal. *Quaestio facti: Revista Internacional sobre Razonamiento Probatorio*, Girona, v. 2, p. 225–250, 2021. https://doi.org/10.33115/udg_bib/qf.i2.22487.

MERRIAM-WEBSTER. *Fishing expedition*. *Merriam-Webster.com Dictionary*, 2020. Disponível em: https://www.merriam-webster.com/dictionary/fishing%20expedition. Acesso em: 16 ago. 2025.

MERRIAM-WEBSTER. *Serendipity*. *Merriam-Webster.com Dictionary*, 2025. Disponível em: https://www.merriam-webster.com/dictionary/serendipity. Acesso em: 20 Aug. 2025.

MINTO, Andressa Olmedo. *A prova digital no processo penal*. São Paulo: LiberArs, 2021.

MOTTA, Débora. Admissibilidade da quebra do sigilo do WhatsApp na investigação criminal: à luz do princípio da privacidade. *Revista da ESMESC*, v. 26, n. 32, p. 113–136, 2019. DOI: http://dx.doi.org/10.14295/revistadaesmesc.v26i32.p113.

NOVELINO, Marcelo. Direito constitucional. 4. ed. Rio de Janeiro: Forense; São Paulo: Método, 2010.

OLIVEIRA, Cássio Roberto Uruga. *A (in)constitucionalidade da prova penal obtida com violação da privacidade nos meios digitais: uma análise sobre os dados de comunicação em aplicativos de mensagens instantâneas*. 2021. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade do Extremo Sul Catarinense, Criciúma, 2021.

PARODI, Lorenzo. A cadeia de custódia da prova digital à luz da Lei 13.968/2019. *Consultor Jurídico*, 18 jun. 2020. Disponível em: https://www.conjur.com.br/2020-jun-18/lorenzo-parodi-cadeia-custodia-prova-digital. Acesso em: 27 jun. 2025

PINHEIRO, Patricia Peck. *Direito digital*. 7. ed. São Paulo: Saraiva Educação, 2021.

PITOMBO, Cleunice A. Valentim Bastos. A desfuncionalização da busca e da apreensão. *Boletim IBCCRIM*, v. 13, n. 151, p. 2–3, jun. 2005.

PITTA, Rafael Gomiero. *Pre-suit e pretrial: as lições do sistema anglo-americano para as necessárias reformas do procedimento probatório brasileiro*. 2019. Tese (Doutorado em Ciência Jurídica) – Universidade Estadual do Norte do Paraná, Jacarezinho, 2019.

PRADO, Geraldo. *Limite às interceptações telefônicas e a jurisprudência do Superior Tribunal de Justiça*. 2. ed. Rio de Janeiro: Lumen Juris, 2006.

QUEIJO, Maria Elizabeth. *O direito de não produzir prova contra si mesmo (o princípio nemo tenetur se detegere e suas decorrências no processo penal)*. São Paulo: Saraiva, 2013.

RAMOS, João Victor Inkis de Mattos. *Fishing expedition e provas ilícitas no processo penal brasileiro: uma análise crítica à luz do Estado Democrático de Direito*. 2021. Monografia (Bacharelado em Direito) – Faculdade de Direito, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2021.

RIBEIRO, Gustavo Alves Magalhães; CORDEIRO, Pedro Ivo Rodrigues Velloso; FUMACH, Débora Moretti. O malware como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 8, n. 3, p. 1463–1500, set.–dez. 2022. Disponível em: https://doi.org/10.22197/rbdpp.v8i3.723. Acesso em: 19 jul.2025

ROSA, Alexandre Morais da. A prática de *fishing expedition* no Processo Penal. *Consultor Jurídico*, São Paulo, 2 jul. 2021. Disponível em: https://www.conjur.com.br/2021-jul-02/limite-penal-pratica-fishingexpedition-processo-penal/. Acesso em: 5 ago. 2025.

ROSA, Alexandre Morais da; SILVA, Viviani Ghizoni; MELO E SILVA, Philipe Benoni. *Fishing Expedition e Encontro Fortuito na busca e apreensão: um dilema oculto do processo penal*. 1. ed. Florianópolis: Emais, 2019.

SAAD GIMENES, Marta C.; ROSSI, Helena C.; PARTATA, Pedro H. A obtenção das provas digitais no processo penal demanda uma disciplina jurídica própria? Uma análise do conceito, das características e das peculiaridades das provas digitais. *Revista Brasileira de Direito Processual Penal*, v. 10, n. 3, e1071, set./dez. 2024. Disponível em: https://doi.org/10.22197/rbdpp.v10i3.1071. Acesso em: 11 jul. 2025.

SILVA, José Afonso da. *Curso de direito constitucional positivo*. 11. ed. São Paulo: Malheiros, 1996.

SILVA, Philipe Benoni Melo e. *Fishing Expedition: a pesca predatória por provas por parte dos órgãos de investigação*. 2017. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/fishingexpedition-20012017. Acesso em: 5 ago. 2025.

SMANIO, Gianluca Martins. *Vigilância policial em meio digital: entre o garantismo e a eficiência*. Curitiba: Juruá, 2022.

SMANIO, Gianpaolo Poggio; KIBRIT, Orly; MANHOSO, Eduardo. Provas digitais e cadeia de custódia: desafios e perspectivas. *Revista Internacional CONSINTER de Direito*, n. 17, p. 141–162, 2023. DOI: 10.19135/revista.consinter.00017.07. Disponível em: https://revistaconsinter.com/index.php/ojs/1707. Acesso em: 9 ago. 2025.

SOARES, Ramon D'Ávila Prottes; OLIVEIRA, Gabriel Fernando Soares. Uma análise do princípio da serendipidade à luz das provas ilícitas no direito processual penal. *Revista Vox*, n. 17, p. 48–58, jan./jun. 2023. ISSN 2359-5183.

THAMAY, Renan; TAMER, Maurício. *Provas no direito digital: conceito da prova digital, procedimentos e provas em espécie*. 2. ed. São Paulo: Thomson Reuters, 2022. p. 33.

ZILLI, Marcos. A prisão em flagrante e o acesso de dados em dispositivos móveis. Nem utopia, nem distopia. Apenas a racionalidade. In: ABREU, Jacqueline de Souza; ANTONIALLI, Dennys (org.). *Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate*. Vol. I. São Paulo: InternetLab, 2018. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2018/08/DIGITAL_InternetLAB_SIMPLES.pdf. Acesso em: 1 jul. 2025.

ZIMIANI, Gustavo Bertho. O fenômeno da serendipidade à luz da jurisprudência do STJ e do STF. *Revista Unigran*, São Paulo, v. 22, n. 43, p. 135–149, jun. 2020.