RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VI, v.1 2025 | submissão: 20/12/2025 | aceito: 23/12/2025 | publicação: 26/12/2025

Inteligência artificial na persecução penal: prova digital, garantias processuais e os limites da investigação criminal no Brasil

Artificial intelligence in criminal prosecution: digital evidence, procedural guarantees and the limits of criminal investigation in Brazil

Ivan Muniz

RESUMO

A incorporação de ferramentas de inteligência artificial e de tecnologias de análise forense digital à investigação criminal tem produzido novas possibilidades para a identificação de autoria, obtenção, extração e análise de evidências digitais. Ao mesmo tempo, a utilização desses recursos suscita questionamentos quanto à proteção dos direitos fundamentais e à observância das garantias processuais asseguradas ao investigado e ao acusado. Nesse contexto, o presente estudo tem como objetivo analisar os limites jurídicos impostos ao emprego de ferramentas tecnológicas baseadas em inteligência artificial na persecução penal brasileira, com especial atenção à prova digital, à cadeia de custódia, à licitude da prova, ao contraditório, à ampla defesa, à presunção de inocência e à necessidade de autorização judicial. Para tanto, foi realizada pesquisa bibliográfica e documental, complementada por levantamento jurisprudencial junto aos Tribunais de Justiça e aos Tribunais Superiores, especialmente o Superior Tribunal de Justiça e o Supremo Tribunal Federal. A análise jurisprudencial identificou decisões envolvendo principalmente a utilização da ferramenta forense digital Cellebrite na investigação de crimes como homicídio e tráfico de drogas. Verificou-se, ainda, a existência de limitada produção jurisprudencial especificamente relacionada ao emprego de inteligência artificial na persecução de crimes cibernéticos, evidenciando uma lacuna relevante no tratamento judicial da matéria. Os resultados indicam que a utilização dessas tecnologias não é, por si só, incompatível com o processo penal, desde que submetida aos limites constitucionais e legais, especialmente quanto à autorização judicial, à preservação da integridade da prova, à transparência dos procedimentos e ao efetivo acesso da defesa aos elementos probatórios. Conclui-se que o avanço tecnológico deve ser acompanhado pelo fortalecimento das garantias processuais, de modo a impedir que a eficiência investigativa se sobreponha aos direitos fundamentais.

Palavras-chave: Inteligência Artificial. Persecução Penal. Prova Digital.

ABSTRACT

The incorporation of artificial intelligence tools and digital forensic technologies into criminal investigations has created new possibilities for identifying perpetrators and obtaining, extracting, and analyzing digital evidence. At the same time, the use of such technologies raises concerns regarding the protection of fundamental rights and compliance with procedural guarantees afforded to suspects and defendants. In this context, this study aims to analyze the legal limits governing the use of technology-based tools and artificial intelligence in Brazilian criminal proceedings, with particular attention to digital evidence, chain of custody, admissibility of evidence, adversarial proceedings, the right to a full defense, the presumption of innocence, and the requirement of judicial authorization. To this end, bibliographic and documentary research was conducted, complemented by a case-law survey involving Brazilian Courts of Justice and Superior Courts, particularly the Superior Court of Justice and the Federal Supreme Court. The case-law analysis identified decisions mainly involving the use of the Cellebrite digital forensic tool in investigations of crimes such as homicide and drug trafficking. The research also revealed limited case law specifically addressing the use of artificial intelligence in the investigation and prosecution of cybercrimes, highlighting a significant gap in the judicial treatment of the subject. The findings indicate that the use of these technologies is not, in itself, incompatible with criminal proceedings, provided that it remains subject to constitutional and statutory safeguards, particularly regarding judicial authorization, preservation of evidentiary integrity, procedural transparency, and effective defense access to evidentiary materials. It is concluded that technological advancement must be accompanied by the strengthening of procedural safeguards in order to prevent investigative efficiency from overriding fundamental rights.

Keywords: Artificial Intelligence. Criminal Prosecution. Digital Evidence.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VI, v.1 2025 | submissão: 20/12/2025 | aceito: 23/12/2025 | publicação: 26/12/2025

1 INTRODUÇÃO

A transformação tecnológica das últimas décadas modificou de maneira significativa as formas de interação social, comunicação, armazenamento de informações e produção de conhecimento. Paralelamente, essas transformações também repercutiram sobre a criminalidade e sobre os mecanismos empregados pelo Estado para sua investigação e persecução. A crescente utilização de dispositivos eletrônicos, plataformas digitais, sistemas informatizados e ambientes virtuais fez com que parcela significativa dos elementos relevantes para a apuração de infrações penais passasse a existir em formato digital, ampliando a importância da prova digital no processo penal contemporâneo.

Nesse cenário, o desenvolvimento de ferramentas de inteligência artificial e de sistemas especializados em análise forense digital passou a oferecer novas possibilidades para a atividade investigativa. Recursos capazes de processar grandes volumes de informações, identificar padrões, organizar dados, recuperar arquivos e auxiliar na análise de dispositivos eletrônicos podem contribuir para conferir maior eficiência à investigação criminal. A utilização dessas tecnologias mostra-se particularmente relevante diante do crescimento da quantidade e da complexidade dos dados produzidos no ambiente digital, circunstância que dificulta a análise exclusivamente manual das informações obtidas durante uma investigação.

Entretanto, a busca por maior eficiência na persecução penal não pode ocorrer de maneira dissociada das garantias fundamentais asseguradas pelo ordenamento jurídico brasileiro. A utilização de tecnologias avançadas para obtenção e tratamento de dados pode atingir diretamente direitos relacionados à intimidade, à vida privada, ao sigilo das comunicações, ao contraditório, à ampla defesa e ao devido processo legal. Por essa razão, a incorporação da inteligência artificial à investigação criminal exige a definição de limites jurídicos capazes de impedir que a eficiência tecnológica se transforme em instrumento de violação de direitos fundamentais.

A Constituição Federal de 1988 estabelece um conjunto de garantias destinadas a limitar o exercício do poder punitivo estatal, entre as quais se destacam o devido processo legal, o contraditório, a ampla defesa, a presunção de inocência e a inadmissibilidade das provas obtidas por meios ilícitos (Brasil, 1988). Tais garantias assumem especial relevância quando a persecução penal envolve tecnologias capazes de acessar, extrair, cruzar e interpretar grandes quantidades de informações provenientes de dispositivos eletrônicos.

A discussão também envolve a própria confiabilidade da prova digital. Diferentemente de determinados elementos probatórios tradicionais, os dados digitais podem ser facilmente copiados, modificados, transferidos ou eliminados, tornando indispensável a adoção de procedimentos destinados a preservar sua autenticidade e integridade. Nesse contexto, a cadeia de custódia constitui importante mecanismo de controle da trajetória do vestígio desde sua identificação até sua utilização no processo, permitindo maior segurança quanto à manutenção das características do elemento probatório.

A utilização de ferramentas de inteligência artificial acrescenta novos desafios a esse cenário. Sistemas

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VI, v.1 2025 | submissão: 20/12/2025 | aceito: 23/12/2025 | publicação: 26/12/2025

automatizados podem auxiliar na localização e organização de informações relevantes, mas seus resultados precisam permanecer sujeitos à fiscalização humana e ao controle jurisdicional. A possibilidade de que mecanismos tecnológicos produzam conclusões a partir de grandes volumes de dados exige transparência suficiente para que os envolvidos no processo possam compreender, questionar e, quando necessário, contestar os elementos utilizados para fundamentar determinada conclusão investigativa.

Nesse sentido, a questão central deste estudo consiste em verificar em que medida o emprego de ferramentas de inteligência artificial e de tecnologias de análise forense digital na persecução penal brasileira pode ser compatibilizado com as garantias processuais asseguradas ao investigado e ao acusado. Busca-se compreender, especialmente, quais limites devem ser observados para que a utilização desses instrumentos não resulte em violação de direitos fundamentais ou em produção probatória incompatível com o devido processo legal.

Para alcançar esse objetivo, a pesquisa foi desenvolvida mediante revisão bibliográfica e documental, abrangendo estudos relacionados à inteligência artificial, à prova digital, à cadeia de custódia e às garantias processuais penais. Também foi realizado levantamento jurisprudencial perante os Tribunais de Justiça e os Tribunais Superiores, com especial atenção às decisões do Superior Tribunal de Justiça e do Supremo Tribunal Federal. Foram utilizadas, entre outras, palavras-chave relacionadas às principais ferramentas de análise forense digital identificadas na literatura e na jurisprudência, como Cellebrite, Peritus, Avilla Forensics, NuDetective, Watson Explorer, Nuix Workstation e Autopsy Forensics.

A pesquisa jurisprudencial revelou número reduzido de decisões que enfrentam diretamente a relação entre inteligência artificial, investigação criminal e garantias processuais, especialmente quando se trata de crimes cibernéticos. Os precedentes localizados concentram-se principalmente na utilização da ferramenta Cellebrite em investigações envolvendo crimes comuns, como homicídio e tráfico de drogas. Embora também tenham sido encontradas decisões relacionadas a crimes cibernéticos, especialmente aqueles previstos no artigo 241-A do Estatuto da Criança e do Adolescente, os recursos analisados não apresentaram como questão central a existência de violação das garantias processuais decorrente do emprego das ferramentas tecnológicas.

Diante desse cenário, o estudo procura contribuir para o debate acerca dos limites jurídicos da utilização da inteligência artificial na persecução penal, considerando que o desenvolvimento tecnológico não elimina a necessidade de observância das garantias fundamentais. Ao contrário, quanto maior for a capacidade estatal de acessar, processar e interpretar informações digitais, maior deverá ser a preocupação com mecanismos de controle, transparência e proteção dos direitos individuais.

Assim, o artigo está estruturado de modo a abordar inicialmente os fundamentos constitucionais e os princípios limitadores do Direito Penal e Processual Penal, passando posteriormente pela análise da prova ilícita, dos limites da persecução penal e da utilização da inteligência artificial na investigação criminal. Em seguida, examina-se a prova digital e os mecanismos de preservação de sua integridade,

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VI, v.1 2025 | submissão: 20/12/2025 | aceito: 23/12/2025 | publicação: 26/12/2025

com destaque para a cadeia de custódia. Por fim, apresenta-se a análise jurisprudencial dos precedentes identificados, buscando compreender como o Poder Judiciário brasileiro vem enfrentando a utilização de ferramentas tecnológicas de investigação e quais parâmetros podem ser extraídos dessas decisões para a proteção das garantias processuais.

2 REFERENCIAL TEÓRICO

2.1 Fundamentos Constitucionais e Princípios Limitadores do Direito Penal e Processual Penal

O Direito Penal desempenha uma função essencial na organização da vida em sociedade, especialmente diante de condutas que atingem de maneira significativa direitos e interesses juridicamente protegidos. Embora diferentes mecanismos de controle social contribuam para a manutenção da ordem e da convivência coletiva, determinadas situações exigem a atuação do Estado por meio do sistema penal, sobretudo quando os demais instrumentos disponíveis não se mostram suficientes para responder à gravidade da lesão produzida. Nesse sentido, a intervenção penal representa uma das formas mais intensas de atuação estatal sobre a esfera individual, circunstância que justifica a existência de limites jurídicos destinados a impedir o exercício arbitrário do poder punitivo (LIMA, 2017).

Essa necessidade de contenção também se manifesta no âmbito do Processo Penal. A persecução penal estatal é desenvolvida mediante uma sucessão ordenada de atos, praticados pelos diferentes sujeitos e órgãos que integram a relação processual, segundo procedimentos previamente estabelecidos pelo ordenamento jurídico. A existência desse aparato processual não representa apenas um instrumento para viabilizar a aplicação da pena, mas também uma garantia contra possíveis abusos decorrentes do exercício do poder estatal. Assim, quanto maior a capacidade de intervenção do Estado sobre os direitos individuais, maior deve ser a exigência de observância das garantias processuais (BADARÓ, 2021).

A partir dessa perspectiva, os princípios penais e processuais penais assumem posição central na estrutura do sistema jurídico. Eles funcionam como parâmetros para a elaboração, interpretação e aplicação das normas, estabelecendo limites à atuação estatal e orientando a atividade dos operadores do Direito. A Constituição Federal, a legislação infraconstitucional e os tratados internacionais de direitos humanos compõem um conjunto normativo que estabelece diretrizes para o funcionamento do sistema punitivo, impondo que a aplicação da sanção penal esteja submetida não apenas às regras jurídicas, mas também aos princípios e postulados que estruturam o Estado de Direito.

Por essa razão, o Direito Penal não pode ser compreendido apenas como um conjunto de dispositivos destinados a definir crimes e estabelecer penas. Sua função também envolve delimitar as condições sob as quais o poder de punir pode ser exercido, alcançando os momentos de imposição, aplicação e execução das sanções. A dimensão limitadora do Direito Penal constitui, portanto, mecanismo de proteção do indivíduo diante da possibilidade de excessos por parte do Estado (BADARÓ, 2021).

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VI, v.1 2025 | submissão: 20/12/2025 | aceito: 23/12/2025 | publicação: 26/12/2025

No mesmo sentido, os princípios e garantias fundamentais constituem elementos indispensáveis à legitimidade da atuação jurisdicional na esfera penal. Além de estruturarem o processo e orientarem a atuação dos sujeitos processuais, essas garantias funcionam como instrumentos de proteção dos direitos individuais, especialmente diante da possibilidade de restrição da liberdade e de outros direitos decorrente da persecução penal. A preservação da dignidade da pessoa humana, nesse cenário, constitui elemento fundamental para que a atividade repressiva estatal permaneça submetida aos limites estabelecidos pelo ordenamento jurídico.

A Constituição Federal de 1988 conferiu especial relevância aos direitos e garantias fundamentais ao dedicar-lhes o Título II. Conforme observa Muniz, esse conjunto constitucional encontra-se organizado em diferentes categorias, abrangendo direitos e garantias individuais e coletivos, direitos sociais, direitos relacionados à nacionalidade, direitos políticos e aqueles referentes à existência, organização e participação em partidos políticos (LIMA, 2017). Essa sistematização evidencia a amplitude da proteção conferida pelo texto constitucional aos indivíduos e à sua participação na estrutura social e política do Estado.

Os direitos fundamentais apresentam, nesse contexto, uma dupla dimensão de atuação. De um lado, possuem caráter defensivo, estabelecendo limites à interferência dos poderes públicos na esfera jurídica dos indivíduos. De outro, apresentam uma dimensão prestacional ou protetiva, impondo ao Estado a adoção de medidas destinadas a prevenir ou impedir violações e danos aos direitos juridicamente assegurados (BADARÓ, 2021). Essa dupla função é especialmente relevante no campo penal, em que a atuação estatal pode produzir restrições intensas sobre direitos individuais. A estrutura constitucional brasileira também contempla princípios expressos e implícitos. Os primeiros encontram previsão direta no texto normativo, enquanto os segundos são identificados a partir da interpretação sistemática do ordenamento jurídico, considerado como uma unidade dotada de coerência e finalidade própria. Dessa maneira, a compreensão das normas constitucionais não se limita à leitura isolada de seus dispositivos, exigindo também a consideração dos princípios que orientam e conferem sentido ao conjunto do sistema jurídico (LANTYER, 2023).

Entretanto, a proteção conferida aos direitos fundamentais não significa que esses direitos possuam caráter absoluto. O Supremo Tribunal Federal reconhece que direitos e garantias fundamentais podem sofrer limitações, especialmente quando entram em tensão com outros direitos ou valores igualmente protegidos constitucionalmente. Não se estabelece, portanto, uma hierarquia geral e previamente definida entre esses direitos, sendo necessário buscar, diante de situações concretas de conflito, uma solução que preserve tanto quanto possível os valores jurídicos envolvidos.

Nessas situações, a atividade interpretativa deve buscar a harmonização dos direitos em conflito. Conforme a doutrina constitucional, a solução não consiste necessariamente na eliminação completa de um dos direitos envolvidos, mas na realização de um juízo de ponderação que considere as particularidades do caso concreto, a intensidade da restrição e os interesses jurídicos em confronto. O

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VI, v.1 2025 | submissão: 20/12/2025 | aceito: 23/12/2025 | publicação: 26/12/2025

objetivo é alcançar uma composição capaz de preservar os valores constitucionais envolvidos na maior medida possível (BADARÓ, 2021). A ponderação, nesse sentido, constitui importante mecanismo para a resolução de conflitos entre princípios e direitos fundamentais. Alves (2022) destaca sua utilização como método de aplicação de princípios tanto na doutrina brasileira quanto na estrangeira. Na perspectiva de Ronald Dworkin, os princípios apresentam uma dimensão de peso, enquanto Robert Alexy diferencia a lógica de funcionamento dos princípios daquela atribuída às regras. A técnica de *balancing*, desenvolvida também na tradição jurídica norte-americana, relaciona-se justamente à necessidade de solucionar conflitos normativos envolvendo valores que não podem ser adequadamente resolvidos apenas pelos métodos tradicionais de interpretação.

A distinção entre princípios e regras também é relevante para a compreensão da estrutura das normas fundamentais. Os princípios possuem função orientadora e servem como fundamentos para a elaboração, interpretação e aplicação das normas jurídicas. As regras, por sua vez, conferem maior concretude aos comandos derivados desses fundamentos, estabelecendo prescrições específicas para determinadas situações (LANTYER, 2023). Dessa relação decorre uma estrutura normativa em que princípios e regras atuam conjuntamente na organização e no funcionamento do sistema jurídico.

Essa compreensão assume especial importância quando aplicada ao Direito Penal e Processual Penal, uma vez que o exercício do poder punitivo estatal deve permanecer permanentemente submetido a limites jurídicos. A definição de condutas criminosas, a investigação, a persecução penal, o julgamento e a eventual aplicação da sanção devem observar não apenas as disposições legais específicas, mas também o conjunto de princípios e garantias que impedem a utilização arbitrária do poder estatal.

Diante dessas premissas, a análise dos crimes cibernéticos exige a consideração de princípios fundamentais capazes de orientar tanto a interpretação das normas penais quanto a própria atuação do Estado diante das novas formas de criminalidade. Embora o ordenamento jurídico disponha de diversos princípios relevantes, a presente abordagem concentra-se naqueles que apresentam maior pertinência para a compreensão dos delitos praticados em ambientes digitais.

Assim, sem a pretensão de esgotar a discussão teórica, serão examinados os princípios fundamentais de natureza material e formal relacionados aos limites da intervenção repressiva estatal, à teoria do delito e à aplicação das sanções penais. A escolha desses fundamentos permite estabelecer uma base teórica para compreender de que maneira o Direito Penal pode responder aos desafios decorrentes da criminalidade cibernética sem afastar as garantias constitucionais que condicionam o exercício do poder de punir.

2.2 Prova Ilícita, Limites da Persecução Penal e Inteligência Artificial na Investigação Criminal

A inadmissibilidade das provas obtidas por meios ilícitos constitui uma importante garantia fundamental

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VI, v.1 2025 | submissão: 20/12/2025 | aceito: 23/12/2025 | publicação: 26/12/2025

prevista no ordenamento jurídico brasileiro. O artigo 5º, inciso LVI, da Constituição Federal estabelece que são inadmissíveis, no processo, as provas obtidas por meios ilícitos. Essa previsão representa uma limitação direta ao poder estatal, uma vez que impede que o Estado, no exercício de sua atividade persecutória, recorra a mecanismos que violem normas jurídicas ou direitos fundamentais para obter elementos destinados à instrução processual. Trata-se, portanto, de uma garantia de caráter negativo, pois impõe aos poderes públicos o dever de se abster de determinadas práticas que possam atingir a esfera jurídica dos indivíduos.

Nesse contexto, Fabiano Augusto Petean e Bruno Cardenal Castilho (2020) destacam que a vedação constitucional às provas ilícitas constitui uma manifestação da proteção dos direitos fundamentais diante da atuação estatal. A regra estabelece um limite à atividade investigativa e processual, impedindo que a busca pela responsabilização criminal seja realizada mediante a violação das próprias garantias que estruturam o Estado de Direito.

A distinção entre provas ilegais, ilegítimas e ilícitas também se mostra relevante para a compreensão do instituto. Conforme explica Gustavo Henrique Badaró (2021), a doutrina brasileira, a partir da distinção formulada por Ada Pellegrini Grinover com fundamento em Nuvolone, compreende as provas contrárias ao ordenamento jurídico como pertencentes ao gênero das provas ilegais. Dentro dessa classificação encontram-se, de um lado, as provas ilegítimas, produzidas mediante violação de normas processuais, e, de outro, as provas ilícitas, obtidas com afronta às normas de direito material ou às garantias previstas constitucionalmente.

A diferença entre essas categorias possui consequências jurídicas relevantes. As provas ilícitas podem decorrer, por exemplo, da violação de direitos fundamentais relacionados às liberdades públicas e aos direitos da personalidade. Nessa perspectiva, quando a obtenção do elemento probatório ocorre mediante afronta a garantias constitucionalmente protegidas, sua utilização no processo encontra obstáculo jurídico justamente porque o Estado não pode legitimar uma atuação investigativa baseada na violação de direitos fundamentais. Badaró (2021) ressalta, nesse sentido, que a proteção alcança bens jurídicos de elevada relevância, cuja violação pode inclusive configurar ilícito penal, como ocorre na obtenção de prova mediante violação de domicílio.

A Constituição Federal, ao estabelecer a inadmissibilidade das provas ilícitas, promove uma articulação entre as normas de direito material e aquelas que disciplinam o processo. Como observa Badaró (2021), a inadmissibilidade pode ser compreendida como uma consequência processual decorrente da violação de uma norma de natureza material. Embora o texto constitucional estabeleça expressamente a proibição, é a legislação processual penal que disciplina de maneira mais específica os efeitos decorrentes da utilização desses elementos no processo.

O artigo 157 do Código de Processo Penal estabelece que as provas ilícitas são inadmissíveis e devem ser desentranhadas do processo. Dessa forma, a consequência não se limita ao reconhecimento abstrato da irregularidade na obtenção da prova, mas alcança sua permanência nos autos e sua utilização como

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VI, v.1 2025 | submissão: 20/12/2025 | aceito: 23/12/2025 | publicação: 26/12/2025

elemento de fundamentação da atividade jurisdicional. A retirada da prova busca impedir que um elemento produzido em desconformidade com o ordenamento jurídico seja utilizado para sustentar validamente a persecução penal (ALMEIDA, 2014).

A vedação também se estende às provas que tenham sido obtidas como consequência de uma prova originalmente ilícita. Essa construção é conhecida como doutrina dos "frutos da árvore envenenada" (*fruit of the poisonous tree*), desenvolvida na tradição jurídica norte-americana. Conforme explica Badaró, a prova derivada pode ser atingida pela ilicitude da prova originária quando existir relação causal entre ambas. Essa consequência, entretanto, comporta exceções quando o vínculo entre a prova inicialmente ilícita e a prova posteriormente obtida é rompido.

Entre as hipóteses tradicionalmente relacionadas à superação dessa contaminação encontram-se a atenuação da mácula (*attenuation of the taint*), a existência de uma fonte independente (*independent source*) e a descoberta inevitável (*inevitable discovery*). Nessas situações, a existência de circunstâncias autônomas capazes de conduzir à obtenção do elemento probatório impede que a ilicitude da prova originária necessariamente contamine o resultado posteriormente alcançado.

No ordenamento jurídico brasileiro, essa matéria recebeu tratamento específico com a Lei nº 11.690/2008, responsável por alterar dispositivos do Código de Processo Penal relacionados à prova. A legislação passou a estabelecer que também são inadmissíveis as provas derivadas das ilícitas, ressalvadas as situações em que não seja demonstrado o nexo de causalidade entre elas ou quando a prova derivada puder ser obtida por uma fonte independente. A própria norma define como fonte independente aquela que, seguindo os procedimentos ordinários e próprios da investigação ou da instrução criminal, seria capaz de conduzir autonomamente ao fato objeto da prova.

A disciplina das provas ilícitas demonstra, portanto, que a atividade persecutória estatal não possui caráter ilimitado. Como destaca Badaró (2021), a existência do poder estatal de investigação e punição deve estar acompanhada de mecanismos jurídicos capazes de impedir que esse poder seja exercido em desacordo com os direitos assegurados pelo próprio ordenamento. A vedação da prova ilícita encontra-se, assim, diretamente relacionada ao devido processo legal e funciona como instrumento de contenção do *jus puniendi*.

Essa preocupação adquire especial importância diante da incorporação crescente de recursos tecnológicos às atividades de investigação criminal. O desenvolvimento de ferramentas digitais ampliou significativamente a capacidade de coleta, armazenamento, cruzamento e análise de informações, proporcionando novas possibilidades para a apuração de delitos complexos. Ao mesmo tempo, essas tecnologias podem produzir riscos adicionais aos direitos fundamentais, especialmente quando utilizadas para acessar, processar ou correlacionar informações pertencentes à esfera privada dos indivíduos.

Entre as tecnologias que passaram a ocupar espaço relevante nesse contexto encontra-se a Inteligência Artificial. Segundo Camel André de Godoy Farah (2019), a Comissão Europeia, em 2018, descreveu a

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VI, v.1 2025 | submissão: 20/12/2025 | aceito: 23/12/2025 | publicação: 26/12/2025

inteligência artificial como um sistema capaz de apresentar comportamento inteligente a partir da análise de seu ambiente e da realização de ações com determinado grau de autonomia, direcionadas ao alcance de objetivos específicos. Esses sistemas podem atuar por meio de softwares destinados, por exemplo, à análise de imagens, ao processamento de dados e ao reconhecimento facial, ou ainda funcionar de maneira integrada a dispositivos de hardware.

A utilização de sistemas inteligentes na investigação criminal decorre, em grande medida, da capacidade dessas ferramentas de processar grandes quantidades de informações e identificar padrões que poderiam ser difíceis de perceber por métodos exclusivamente convencionais. Farah (2019) ressalta a importância da evolução tecnológica e dos sistemas inteligentes, destacando seu potencial de utilização na análise de fenômenos complexos e na busca de soluções aplicáveis a situações concretas.

No âmbito criminal, a inteligência artificial pode, portanto, assumir função auxiliar na atividade investigativa, contribuindo para a identificação e análise de informações relevantes à apuração de delitos. Seu emprego pode ser particularmente significativo em investigações envolvendo ambientes digitais, nos quais o volume de dados e a velocidade de circulação das informações tornam os métodos tradicionais de análise cada vez mais limitados. A tecnologia passa, assim, a integrar os instrumentos disponíveis para a atuação do sistema penal em sua função de repressão aos delitos, observada a característica de última *ratio* atribuída ao Direito Penal (ALMEIDA, 2014).

Entretanto, a capacidade tecnológica de produzir ou localizar informações não significa que todo elemento obtido por meio desses mecanismos possa ser automaticamente utilizado como prova. A inovação tecnológica não afasta as exigências constitucionais e processuais que condicionam a validade da atividade investigativa. Ao contrário, a utilização de ferramentas capazes de ampliar significativamente o poder de vigilância, identificação e processamento de informações exige especial atenção aos limites impostos pelos direitos fundamentais.

Nesse sentido, a aplicação da inteligência artificial na investigação criminal deve ser compatibilizada com as garantias que estruturam o processo penal. A busca por maior eficiência na apuração dos crimes não pode servir como justificativa para relativizar indiscriminadamente a privacidade, a intimidade, o devido processo legal ou as demais garantias constitucionalmente asseguradas. A tecnologia deve funcionar como instrumento de apoio à investigação, e não como mecanismo capaz de afastar os limites jurídicos impostos ao exercício do poder estatal (FONTENELE; HOMSI; GONÇALVES, 2021).

Essa questão torna-se ainda mais relevante diante da expansão dos crimes cibernéticos. A natureza digital de determinadas infrações faz com que a investigação dependa, cada vez mais, de ferramentas capazes de localizar, preservar, organizar e interpretar grandes volumes de informações. Ao mesmo tempo, a obtenção desses dados deve observar critérios de legalidade, de modo que a eficiência investigativa não resulte na produção de provas posteriormente consideradas ilícitas.

Dessa maneira, o desenvolvimento tecnológico introduz novas possibilidades para a persecução penal, mas também impõe novos desafios à proteção dos direitos fundamentais. A utilização da inteligência

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VI, v.1 2025 | submissão: 20/12/2025 | aceito: 23/12/2025 | publicação: 26/12/2025

artificial, do reconhecimento facial, da análise automatizada de dados e de outras ferramentas digitais deve estar subordinada aos princípios que limitam a atuação estatal. A legitimidade da investigação não depende exclusivamente de sua capacidade de alcançar resultados, mas também da observância dos procedimentos e garantias que conferem validade jurídica aos elementos obtidos (ALMEIDA, 2014).

A relação entre tecnologia, prova e persecução penal evidencia, assim, a necessidade de conciliar eficiência investigativa e proteção das garantias individuais. No enfrentamento da criminalidade contemporânea, especialmente dos crimes praticados em ambientes digitais, os recursos tecnológicos podem representar instrumentos importantes para o Estado. Contudo, sua utilização somente se mostra juridicamente legítima quando permanece submetida aos limites constitucionais e processuais que impedem que a busca pela punição transforme a própria atividade investigativa em fonte de violação de direitos.

2.3 A Prova Digital no Processo Penal

A prova ocupa posição fundamental no processo penal, uma vez que constitui instrumento destinado a fornecer elementos para a reconstrução dos fatos submetidos à apreciação judicial. No ordenamento jurídico brasileiro, sua utilização encontra respaldo constitucional, inclusive no conjunto de garantias relacionadas à proteção do indivíduo diante da persecução penal. O artigo 5º, inciso LXIII, da Constituição Federal assegura ao preso, entre outros direitos, a possibilidade de permanecer em silêncio, estabelecendo importante garantia contra a autoincriminação. Essa proteção também encontra correspondência no artigo 8º, § 2º, alínea “g”, da Convenção Americana sobre Direitos Humanos, promulgada no Brasil pelo Decreto nº 678/1992, que assegura ao acusado o direito de não ser obrigado a depor contra si mesmo nem a declarar-se culpado.

O direito à prova, entretanto, não se limita à possibilidade de apresentar determinado elemento perante o Poder Judiciário. Conforme explica Lantyer (2023), a garantia compreende também a possibilidade de requerer a produção probatória, manifestar-se sobre os elementos apresentados no processo e obter sua efetiva apreciação pelo órgão julgador. A atividade probatória, portanto, está diretamente relacionada ao contraditório e à ampla defesa, exigindo que as partes disponham de condições adequadas para participar da formação do conjunto probatório.

Quanto à relação estabelecida entre a prova e o fato que se pretende demonstrar, Lantyer (2023) diferencia as provas diretas das indiretas. A primeira possui relação imediata com o acontecimento submetido à demonstração, como ocorre, por exemplo, no depoimento de uma testemunha que presenciou determinado fato. A segunda, por sua vez, relaciona-se inicialmente a um acontecimento distinto daquele que se busca comprovar, mas permite, mediante raciocínio lógico, estabelecer uma conclusão sobre o fato principal. Um laudo pericial que analisa a posição dos veículos após um acidente pode ilustrar essa segunda modalidade, pois os elementos observados permitem formular conclusões

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VI, v.1 2025 | submissão: 20/12/2025 | aceito: 23/12/2025 | publicação: 26/12/2025

sobre a dinâmica do acontecimento.

Renato Brasileiro de Lima (2017) propõe ainda a compreensão da prova a partir de três perspectivas complementares: como atividade probatória, como resultado e como meio. Na primeira acepção, a prova corresponde ao conjunto de atos e instrumentos utilizados pelas partes para demonstrar perante o julgador a veracidade de suas alegações. Nessa dimensão, o direito à prova integra as garantias fundamentais relacionadas à ação, à defesa e ao contraditório, de modo que sua restrição indevida pode comprometer o exercício efetivo da defesa ou da acusação.

A prova também pode ser compreendida como resultado da atividade desenvolvida durante o processo. Nesse caso, refere-se à formação da convicção do julgador acerca da existência ou inexistência de determinado fato. Embora a reconstrução processual não permita reproduzir integralmente acontecimentos passados, a atividade probatória busca fornecer elementos suficientes para estabelecer uma conclusão juridicamente adequada acerca da situação discutida. Por fim, a prova como meio corresponde aos instrumentos empregados para possibilitar a formação dessa convicção judicial (Lima, 2017).

A evolução tecnológica, contudo, modificou significativamente o cenário tradicional da produção probatória. A incorporação da tecnologia da informação às atividades cotidianas e o crescimento da criminalidade praticada em ambientes digitais fizeram surgir novas formas de obtenção e preservação de elementos probatórios. Nesse contexto, a investigação criminal passou a depender, em determinadas situações, de informações armazenadas ou transmitidas por dispositivos eletrônicos e redes de comunicação.

Fontenele, Homsi e Gonçalves (2021) destacam que a produção da prova deve permanecer submetida aos requisitos de legalidade e não pode resultar na violação de garantias constitucionais ou infraconstitucionais. Os autores também distinguem provas típicas e atípicas, situando as provas digitais entre estas últimas, uma vez que sua utilização não decorre necessariamente de uma previsão legislativa específica destinada a cada modalidade de dado eletrônico. Ainda assim, sua utilização processual pode ser admitida como instrumento para alcançar fontes de prova e esclarecer questões fáticas relevantes para a solução da controvérsia.

A presença das provas digitais no processo penal tornou-se, dessa forma, cada vez mais expressiva. O Projeto de Lei nº 4.939/2020, apresentado na Câmara dos Deputados, buscou estabelecer diretrizes específicas para a obtenção e admissibilidade desses elementos na investigação e no processo. De acordo com a proposta, prova digital corresponde à informação armazenada ou transmitida por meio eletrônico que apresente valor probatório. O projeto também diferencia a prova originalmente produzida em ambiente eletrônico, denominada prova nato-digital, daquela que teve origem em suporte físico e posteriormente foi convertida para formato eletrônico (Brasil, 2020).

Embora existam tentativas de estabelecer uma definição normativa, a conceituação da prova digital ainda apresenta diferentes perspectivas na literatura especializada. Casey (2011), a partir da doutrina

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VI, v.1 2025 | submissão: 20/12/2025 | aceito: 23/12/2025 | publicação: 26/12/2025

estrangeira, compreende a evidência digital como os dados armazenados ou transmitidos por computadores que possam contribuir para confirmar ou refutar determinada hipótese acerca de um delito ou esclarecer elementos relevantes para sua compreensão, como a intenção ou a existência de um álibi. Em perspectiva semelhante, Vaz (2012) define a prova digital como o conjunto de dados registrados em formato digital, armazenados em dispositivos eletrônicos ou transmitidos por redes de comunicação, capazes de representar fatos ou informações relevantes à investigação. Nessa perspectiva, arquivos armazenados em computadores, telefones celulares, servidores ou outros ambientes digitais podem constituir fontes relevantes para a reconstrução dos acontecimentos investigados.

Almeida (2014) ressalta que a natureza digital do elemento probatório não elimina a necessidade de que ele possua valor probatório suficiente para ser submetido à apreciação judicial. A principal particularidade está justamente em seu suporte e em sua forma de armazenamento ou transmissão, que permitem que a informação seja preservada e compartilhada por diferentes dispositivos e ambientes tecnológicos.

A amplitude das fontes de prova digital é significativa. Lantyer (2023) relaciona entre esses elementos fotografias, vídeos, registros de mensagens, informações obtidas em sites e softwares, metadados, dados provenientes de Estações Rádio Base (ERB) e informações extraídas de smartphones, tablets, computadores portáteis e outros dispositivos eletrônicos. Em razão da natureza desses elementos, o autor destaca a importância dos metadados e da documentação dos procedimentos empregados durante sua coleta e preservação, permitindo verificar posteriormente sua autenticidade e integridade.

As fontes utilizadas para obtenção de evidências digitais podem ser agrupadas, de maneira geral, em fontes abertas e fontes fechadas. As primeiras correspondem às informações disponíveis publicamente na Internet, como conteúdos publicados em sites, mecanismos de pesquisa, portais de notícias e redes sociais, desde que seu acesso ocorra dentro dos limites legais. As fontes fechadas, por outro lado, dependem de procedimentos específicos e, em determinadas situações, de autorização judicial, como ocorre na apreensão e análise de dispositivos eletrônicos protegidos ou na obtenção de determinados dados armazenados em sistemas informáticos (Lantyer, 2023).

O Projeto de Lei nº 4.939/2020 relaciona diferentes mecanismos destinados à obtenção da prova digital, entre eles a busca e apreensão de dispositivos eletrônicos e sistemas informáticos, a coleta remota de dados, a interceptação telemática, o acesso forçado a sistemas ou redes e o tratamento de informações disponibilizadas em fontes abertas (Brasil, 2020). A proposta também prevê cuidados técnicos destinados à preservação da integridade, completude, autenticidade, auditabilidade e reprodutibilidade dos procedimentos empregados.

A exigência de conhecimentos técnicos específicos para a coleta dessas informações, entretanto, suscita discussões. Ferreira (2021) questiona a ideia de restringir determinados procedimentos exclusivamente à atuação de peritos oficiais ou assistentes técnicos da área de informática, considerando que as estruturas de investigação policial podem contar com equipes multidisciplinares. Nesse contexto,

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VI, v.1 2025 | submissão: 20/12/2025 | aceito: 23/12/2025 | publicação: 26/12/2025

agentes com diferentes formações e atribuições podem participar de diligências relacionadas à coleta e preservação de informações, desde que devidamente capacitados e investidos das competências necessárias para a execução das respectivas atividades.

Outro aspecto que diferencia a prova digital dos meios probatórios tradicionais está relacionado às suas características próprias. Minto (2021) destaca a imaterialidade, a volatilidade, a fragilidade e a dispersão como elementos particularmente relevantes. Os dados digitais não dependem de um suporte físico específico para existir e podem ser transferidos entre diferentes dispositivos sem que sua natureza informacional seja alterada. Essa característica, contudo, também amplia sua vulnerabilidade, pois os dados podem ser modificados, apagados ou destruídos com relativa facilidade.

A dispersão constitui igualmente um desafio. Uma determinada informação pode encontrar-se distribuída entre dispositivos, servidores, sistemas de armazenamento remoto, serviços de computação em nuvem, caixas de correio eletrônico e diferentes plataformas digitais, inclusive localizadas em países distintos. Essa característica dificulta a identificação da fonte, a coleta e a preservação dos elementos relevantes, especialmente quando a investigação envolve múltiplos ambientes tecnológicos.

Diante dessas particularidades, consolidou-se a necessidade de procedimentos específicos para identificação, coleta, preservação, análise e apresentação das evidências digitais. A ciência forense digital desempenha, nesse cenário, papel relevante ao desenvolver métodos destinados a assegurar que os dados obtidos durante uma investigação possam ser submetidos posteriormente à apreciação judicial com o maior grau possível de confiabilidade. Fidalgo (2022) observa que a expansão do armazenamento digital e sua crescente presença nas atividades cotidianas contribuíram simultaneamente para o aumento das solicitações de análise forense e para o crescimento exponencial do volume de informações que precisam ser examinadas.

A admissibilidade da prova digital está diretamente relacionada à demonstração de sua autenticidade e à preservação das garantias processuais. Lantyer (2023) ressalta que esses elementos podem ser utilizados perante o Poder Judiciário desde que observados o contraditório, a ampla defesa e os mecanismos destinados à verificação de sua autenticidade. O Código de Processo Civil também contempla regras relacionadas à utilização de documentos eletrônicos e de reproduções de diferentes naturezas como meios aptos à demonstração de fatos, desde que observados os requisitos legais de autenticidade e confiabilidade (Brasil, 2015).

Nesse processo de validação, determinadas tecnologias podem auxiliar na preservação das características originais dos dados. Lantyer (2023) menciona, por exemplo, o emprego de soluções tecnológicas capazes de coletar informações provenientes de diferentes fontes, como imagens, vídeos, mensagens, redes sociais e correios eletrônicos, organizando-as em relatórios técnicos acompanhados dos respectivos metadados. A utilização de mecanismos de autenticação e de assinaturas criptográficas também pode contribuir para conferir maior segurança e confiabilidade aos documentos eletrônicos, inclusive mediante o emprego da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VI, v.1 2025 | submissão: 20/12/2025 | aceito: 23/12/2025 | publicação: 26/12/2025

A utilização das provas digitais apresenta vantagens importantes para a investigação criminal, especialmente pela capacidade de reunir grandes volumes de informações e permitir análises mais rápidas e abrangentes. Entretanto, a facilidade de manipulação constitui uma das principais preocupações relacionadas a esses elementos. No contexto dos crimes cibernéticos, criminosos podem utilizar recursos destinados a ocultar sua identidade, modificar informações ou eliminar vestígios, dificultando tanto a identificação da autoria quanto a reconstrução da materialidade delitiva.

Freitas, Silva e Souza (2023) destacam justamente que a investigação de crimes cibernéticos enfrenta dificuldades relacionadas à volatilidade do ambiente virtual e à possibilidade de alteração ou eliminação das evidências. A identificação do responsável pela conduta constitui um dos principais desafios, pois a existência de informações digitais não significa necessariamente que seja simples estabelecer, de maneira segura, a correspondência entre determinado dado e a pessoa que efetivamente praticou o delito.

A preservação da cadeia de custódia assume, nesse cenário, importância fundamental. O artigo 158-A do Código de Processo Penal, introduzido pela Lei nº 13.964/2019, define a cadeia de custódia como o conjunto de procedimentos destinados a preservar e documentar a trajetória cronológica do vestígio, permitindo acompanhar sua posse e seu manuseio desde o reconhecimento até o descarte (Brasil, 1941). No caso das evidências digitais, essa preocupação torna-se ainda mais relevante em razão da facilidade de alteração, reprodução e transferência dos dados.

Prado (2021) compreende a cadeia de custódia como mecanismo destinado a preservar a integridade do elemento probatório e assegurar sua autenticidade. A observância desse percurso constitui elemento relevante para a avaliação da confiabilidade da prova, uma vez que permite verificar de que maneira o vestígio foi identificado, coletado, transportado, armazenado, analisado e apresentado no processo.

A preservação da integridade dos dados digitais pode contar, ainda, com recursos tecnológicos específicos. Lordelo (2024) destaca o emprego de ferramentas de *hashing*, que produzem um código único associado ao conjunto de dados submetido ao procedimento. A comparação entre o código obtido inicialmente e aquele calculado posteriormente permite identificar eventual alteração no conteúdo analisado. Dessa maneira, o *hash* funciona como mecanismo de verificação da integridade da evidência digital, permitindo detectar modificações realizadas após sua coleta.

A utilização desse recurso apresenta especial relevância quando aplicada a dispositivos eletrônicos, como smartphones e computadores. Uma vez calculado o código correspondente ao conteúdo coletado, qualquer modificação posterior nos dados poderá resultar em um código diferente, permitindo identificar a ocorrência de alterações. O mecanismo contribui, assim, para a preservação da confiabilidade da evidência e para o controle da cadeia de custódia (Lordelo, 2024).

A crescente utilização de documentos e dados digitais como elementos probatórios demonstra a necessidade de adoção de procedimentos capazes de garantir sua integridade, autenticidade e segurança. Embora o ordenamento jurídico brasileiro tenha avançado na incorporação de mecanismos relacionados à prova digital, ainda permanecem desafios decorrentes da velocidade com que as tecnologias se

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VI, v.1 2025 | submissão: 20/12/2025 | aceito: 23/12/2025 | publicação: 26/12/2025

desenvolvem e da diversidade de formatos e ambientes nos quais as informações podem ser produzidas e armazenadas.

Nesse contexto, a ausência de procedimentos uniformes pode dificultar a coleta e a preservação das evidências, especialmente em investigações envolvendo crimes cibernéticos. A necessidade de regulamentação e padronização decorre da necessidade de assegurar que os elementos apresentados ao Poder Judiciário mantenham condições suficientes de autenticidade e integridade.

A problemática torna-se ainda mais complexa quando se considera que, nos crimes praticados em ambientes digitais, a prova eletrônica pode constituir um dos principais, ou mesmo o único, elementos capazes de demonstrar a materialidade e auxiliar na identificação da autoria. Por essa razão, a coleta inadequada, a ausência de documentação ou a alteração não identificada de determinado dado podem comprometer significativamente a investigação.

Dessa maneira, a prova digital deve ser compreendida como um instrumento relevante para o enfrentamento da criminalidade contemporânea, mas sua utilização exige procedimentos técnicos e jurídicos compatíveis com suas características específicas. A eficiência proporcionada pelas tecnologias digitais precisa estar acompanhada de mecanismos capazes de assegurar a autenticidade, a integridade e a rastreabilidade dos elementos obtidos.

A consolidação de métodos de investigação forense, a adequada documentação da cadeia de custódia e o emprego de ferramentas tecnológicas de verificação, como o *hashing*, constituem mecanismos importantes para aumentar a confiabilidade das evidências digitais. Ao mesmo tempo, a evolução normativa permanece necessária para estabelecer parâmetros mais claros e uniformes para a produção, preservação e utilização desses elementos no processo penal.

Assim, o desafio contemporâneo não consiste apenas em ampliar a capacidade estatal de localizar e analisar informações digitais, mas em garantir que essa atividade seja desenvolvida dentro dos limites constitucionais e processuais. A prova digital somente alcança sua plena relevância no processo penal quando, além de contribuir para a reconstrução dos fatos, preserva as garantias fundamentais que sustentam a legitimidade da própria persecução penal.

2.4 Inteligência Artificial na Investigação Criminal: Garantias Processuais e Admissibilidade da Prova Digital

A incorporação de ferramentas de inteligência artificial às atividades relacionadas à investigação de crimes cibernéticos tem provocado novas discussões acerca dos limites da atuação estatal e da preservação das garantias processuais penais. A utilização de sistemas capazes de processar grandes volumes de informações, identificar padrões e extrair dados de dispositivos eletrônicos amplia consideravelmente as possibilidades de investigação, mas também exige atenção quanto aos impactos produzidos sobre direitos fundamentais. Nesse cenário, a legitimidade do emprego dessas tecnologias

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VI, v.1 2025 | submissão: 20/12/2025 | aceito: 23/12/2025 | publicação: 26/12/2025

depende da compatibilização entre eficiência investigativa e respeito às garantias asseguradas pelo ordenamento jurídico.

A crescente complexidade da criminalidade digital contribui para tornar a tecnologia um componente cada vez mais relevante da atividade investigativa. Conforme Stoykova (2021), a ciência forense digital e os mecanismos tecnológicos de obtenção de evidências assumem importância crescente diante do aumento do volume de informações envolvidas nas investigações criminais. A atividade investigativa passa, assim, a demandar métodos capazes de lidar com grandes quantidades de dados e com vestígios que podem apresentar características distintas daqueles encontrados na criminalidade tradicional.

Apesar das vantagens proporcionadas por essas ferramentas, sua utilização também suscita questionamentos relacionados à privacidade e aos direitos individuais. Alves (2022) chama atenção para os riscos decorrentes da utilização de mecanismos tecnológicos capazes de coletar e analisar grandes quantidades de dados pessoais. Quando empregados sem critérios adequados, esses recursos podem ampliar excessivamente a vigilância sobre os indivíduos e produzir interferências desproporcionais na intimidade. A utilização de algoritmos para análise de informações, portanto, deve observar limites jurídicos que impeçam a transformação da eficiência tecnológica em instrumento de vigilância indiscriminada.

A preocupação também alcança a presunção de inocência. Stoykova (2021) aponta que investigações apoiadas por tecnologias digitais podem gerar problemas quando não são acompanhadas de procedimentos adequados, especialmente diante da possibilidade de construção paralela de fatos, utilização de evidências incompletas ou pouco confiáveis, restrição ao acesso da defesa aos elementos probatórios e manutenção prolongada de dados pertencentes a pessoas submetidas à investigação ou utilizadas para fins de comparação. Esses fatores podem comprometer o equilíbrio processual e dificultar o exercício efetivo dos direitos do acusado.

A existência desses riscos, entretanto, não significa que a utilização de ferramentas tecnológicas para obtenção de provas digitais seja necessariamente incompatível com as garantias fundamentais. A jurisprudência brasileira tem admitido, em determinadas circunstâncias, a utilização de tecnologias destinadas à extração e análise de dados armazenados em dispositivos eletrônicos, desde que sejam observados os requisitos jurídicos pertinentes e, quando exigido, exista autorização judicial.

Um exemplo encontra-se na Apelação Criminal nº 0800985-17.2023.8.12.0002, julgada pela 2ª Câmara Criminal do Tribunal de Justiça do Estado de Mato Grosso do Sul, em 29 de agosto de 2023. Na ocasião, o tribunal examinou a utilização da plataforma Cellebrite para extração de informações armazenadas no aparelho celular do acusado e reconheceu a admissibilidade dos elementos obtidos, considerando a existência de autorização judicial para a realização do procedimento (Tribunal de Justiça do Estado de Mato Grosso do Sul, 2023).

O entendimento adotado pelo TJMS partiu da constatação de que o acesso ao conteúdo do dispositivo eletrônico ocorreu mediante autorização judicial. Dessa maneira, o tribunal afastou a alegação de

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VI, v.1 2025 | submissão: 20/12/2025 | aceito: 23/12/2025 | publicação: 26/12/2025

violação à intimidade e à vida privada e não reconheceu a existência de nulidade decorrente da utilização da ferramenta. O caso demonstra que a tecnologia empregada para obtenção dos dados não constitui, isoladamente, fundamento suficiente para invalidar a prova, sendo necessário verificar as circunstâncias concretas em que ocorreu o acesso às informações.

A discussão também chegou ao Supremo Tribunal Federal. No Agravo Regimental na Reclamação nº 33.727, do Estado de Goiás, julgado em 6 de maio de 2019, sob relatoria do Ministro Alexandre de Moraes, foi analisada situação relacionada à utilização da plataforma Cellebrite para obtenção e compartilhamento de informações extraídas de aparelhos celulares apreendidos durante investigação criminal (Supremo Tribunal Federal, 2019).

Naquele caso, a defesa questionou a extensão do acesso às informações obtidas por meio da ferramenta, sustentando que os autos continham apenas capturas de tela e relatórios elaborados pelos agentes responsáveis pela investigação. Argumentou-se que a ausência de acesso integral aos dados poderia comprometer garantias constitucionais e processuais, especialmente o exercício da defesa e a possibilidade de contestação dos elementos utilizados contra o acusado.

Ao analisar a controvérsia, o Supremo Tribunal Federal entendeu que não havia violação às garantias alegadas, considerando que a defesa havia recebido acesso à documentação necessária e que os elementos relevantes estavam disponíveis para consulta. O entendimento reafirmou, portanto, que a utilização de ferramentas tecnológicas para obtenção de dados não implica automaticamente violação ao devido processo legal, desde que sejam preservadas as condições necessárias ao exercício da defesa (Supremo Tribunal Federal, 2019).

Outra discussão relevante foi examinada pelo STF na Reclamação nº 49.369/RS, julgada em 2021 sob relatoria do Ministro Ricardo Lewandowski. A controvérsia envolvia a utilização da ferramenta Cellebrite Physical Analyzer para análise de informações extraídas de dispositivos eletrônicos e a alegação defensiva de impossibilidade de acesso a determinados arquivos de conversas criptografadas. A defesa buscava, entre outros aspectos, questionar a validade das evidências utilizadas no processo (Supremo Tribunal Federal, 2021).

No caso, a controvérsia estava relacionada também à prisão preventiva, fundamentada nos artigos 312 e 313 do Código de Processo Penal, e à alegação de que os elementos digitais utilizados na decisão teriam sido obtidos a partir de informações armazenadas em serviços de nuvem sem a correspondente busca e apreensão no dispositivo pertencente ao investigado.

O Supremo Tribunal Federal, contudo, considerou que a utilização da ferramenta forense empregada pela Polícia Federal não era, por si só, capaz de comprometer a validade dos elementos obtidos. A decisão destacou que o Cellebrite Physical Analyzer constitui uma das ferramentas disponíveis para a análise de grandes volumes de informações provenientes de empresas de tecnologia, permitindo a leitura, organização e categorização de dados por meio de procedimentos parcialmente automatizados (Supremo Tribunal Federal, 2021).

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VI, v.1 2025 | submissão: 20/12/2025 | aceito: 23/12/2025 | publicação: 26/12/2025

Também foi afastada a alegação de violação à Súmula Vinculante nº 14. Segundo o entendimento registrado no julgamento, o acesso a materiais provenientes de medidas de quebra de sigilo pode ser realizado por meio de softwares disponíveis no mercado, não sendo necessária a utilização de mecanismos exclusivos ou de chaves especiais para o processamento de determinados dados criptografados. O ponto central, portanto, não estaria na ferramenta utilizada, mas na observância das garantias processuais e no acesso da defesa aos elementos pertinentes.

A decisão reforça a compreensão de que o emprego de recursos tecnológicos na investigação criminal não conduz automaticamente à invalidade da prova. A legitimidade do procedimento deve ser analisada a partir da forma como a informação foi obtida, dos limites jurídicos impostos à investigação e das condições oferecidas à defesa para conhecer e questionar os elementos utilizados no processo. Nesse sentido, o uso de ferramentas tecnológicas pode coexistir com o devido processo legal quando acompanhado de transparência e respeito às garantias processuais.

Também o Superior Tribunal de Justiça enfrentou questão semelhante no Agravo em Recurso Especial nº 2.083.614/SC, julgado em 12 de fevereiro de 2023, sob relatoria do Ministro Reynaldo Soares da Fonseca. Naquele processo, a defesa alegou nulidade decorrente de cerceamento de defesa e suposta quebra da cadeia de custódia, questionando a suficiência dos elementos relacionados à autoria e à materialidade dos delitos investigados (Superior Tribunal de Justiça, 2023).

No caso analisado pelo STJ, havia determinação judicial para apreensão dos aparelhos celulares dos investigados e posterior extração de dados mediante utilização da plataforma Cellebrite. A decisão também considerou que a defesa tinha conhecimento dos elementos obtidos ao longo da investigação, circunstância relevante para a análise da alegação de violação às garantias processuais (Superior Tribunal de Justiça, 2023).

A análise conjunta desses precedentes permite observar que a jurisprudência brasileira não estabelece uma incompatibilidade absoluta entre inteligência artificial, ferramentas forenses digitais e processo penal. Alves (2022) sustenta que não existe impedimento, em princípio, para a incorporação de instrumentos tecnológicos ao procedimento penal, desde que sua utilização seja submetida a parâmetros jurídicos capazes de proteger os direitos fundamentais envolvidos.

Essa possibilidade, entretanto, não elimina os riscos associados à utilização de tecnologias automatizadas na produção e análise de provas. Fidalgo (2022) ressalta a necessidade de assegurar, especialmente, o contraditório e a ampla defesa. A efetividade desses princípios pressupõe que o acusado tenha condições concretas de conhecer e contestar os elementos utilizados contra si. Quando ferramentas tecnológicas produzem ou organizam informações que servem de fundamento para uma acusação, é necessário garantir que o conteúdo relevante possa ser efetivamente examinado pela defesa.

A questão torna-se ainda mais sensível diante de sistemas cuja operação não seja facilmente compreensível pelos sujeitos processuais. A adoção de mecanismos transparentes e explicáveis constitui uma forma de reduzir esse problema, pois permite compreender os procedimentos utilizados e as razões

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VI, v.1 2025 | submissão: 20/12/2025 | aceito: 23/12/2025 | publicação: 26/12/2025

que conduziram a determinada conclusão. Fidalgo (2022) destaca que a explicabilidade das ferramentas de inteligência artificial contribui para tornar o processo de obtenção e análise das evidências mais acessível, favorecendo o controle e a contestação dos resultados apresentados.

A transparência tecnológica assume, portanto, função diretamente relacionada ao exercício da defesa. Não basta que o Estado disponha de uma ferramenta capaz de produzir determinado resultado; é necessário que existam condições para verificar a maneira pela qual esse resultado foi alcançado e avaliar a confiabilidade dos elementos apresentados. A impossibilidade de compreender ou questionar a origem de uma evidência pode comprometer a efetividade do contraditório.

Essa preocupação também se relaciona à presunção de inocência. Conforme Branco (2021), a utilização de meios digitais de obtenção de prova deve respeitar as garantias processuais que impedem que o acusado seja colocado em posição de desvantagem diante de mecanismos de investigação cuja complexidade técnica dificulte sua contestação. Em situações de dúvida razoável, a proteção decorrente da presunção de inocência também se projeta sobre a avaliação dos elementos utilizados para sustentar a acusação.

Por essa razão, o emprego de ferramentas tecnológicas na investigação criminal exige um equilíbrio entre a necessidade de combater formas contemporâneas de criminalidade e a preservação dos direitos individuais. A utilização de recursos capazes de acessar, processar e correlacionar grandes quantidades de dados pode aumentar a eficiência da investigação, mas também amplia o potencial de interferência na privacidade e na esfera jurídica dos indivíduos.

A criação de mecanismos específicos para preservação da cadeia de custódia digital constitui outro aspecto indispensável. A confiabilidade da evidência depende da tecnologia empregada em sua extração, da documentação e da rastreabilidade de todas as etapas pelas quais o dado passou até sua apresentação ao magistrado. A adoção de procedimentos capazes de demonstrar a autenticidade, a integridade e a origem das informações contribui para reduzir questionamentos acerca de sua validade.

Nesse sentido, Steffen (2022) ressalta que a inteligência artificial não deve ser considerada problemática por sua própria natureza. A questão central está em estabelecer condições para que sua criação, implementação e utilização ocorram dentro de parâmetros de respeito aos direitos humanos e às garantias reconhecidas pelo ordenamento jurídico. A regulamentação, embora importante, deve estar acompanhada de princípios capazes de orientar todo o ciclo de funcionamento dessas ferramentas.

No contexto brasileiro analisado, observa-se que a utilização de tecnologias como o Cellebrite tem sido admitida pelos tribunais em determinadas situações, quando há autorização judicial e quando são preservadas as condições necessárias ao exercício da defesa. Os precedentes examinados indicam que a ferramenta tecnológica considerada não determina a ilicitude ou a validade da prova. O elemento decisivo está relacionado à legalidade da obtenção, à preservação da integridade dos dados e à garantia de acesso aos elementos relevantes do processo.

Assim, a incorporação da inteligência artificial e de ferramentas forenses digitais à investigação criminal

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VI, v.1 2025 | submissão: 20/12/2025 | aceito: 23/12/2025 | publicação: 26/12/2025

representa uma importante transformação nos mecanismos de enfrentamento da criminalidade cibernética. Contudo, a inovação tecnológica deve permanecer subordinada aos princípios que estruturam o processo penal. Eficiência, rapidez e capacidade de processamento não podem substituir os requisitos de legalidade, transparência, contraditório, ampla defesa e respeito à presunção de inocência.

A análise dos julgados mencionados demonstra, portanto, uma tendência de reconhecimento da possibilidade de utilização dessas tecnologias no processo penal, desde que observadas as garantias fundamentais. O desafio jurídico contemporâneo consiste em assegurar que o avanço dos instrumentos de investigação seja acompanhado por mecanismos suficientes de controle, transparência e responsabilização, evitando que a busca pela eficiência na repressão aos crimes cibernéticos resulte na fragilização das garantias que legitimam a própria atuação do sistema de justiça criminal.

2.5 Pesquisa jurisprudencial sobre o uso de ferramentas de inteligência artificial na persecução penal

Com o propósito de aprofundar a análise jurisprudencial acerca da utilização de ferramentas de inteligência artificial na persecução penal, foi realizada pesquisa junto aos Tribunais de Justiça e aos Tribunais Superiores, o Superior Tribunal de Justiça (STJ) e o Supremo Tribunal Federal (STF). A investigação buscou identificar decisões judiciais envolvendo situações concretas nas quais recursos tecnológicos baseados em inteligência artificial ou ferramentas de análise forense digital tenham sido empregados na investigação e persecução de infrações penais no Brasil. Buscou-se verificar a existência de controvérsias submetidas à apreciação judicial nas quais a defesa tenha questionado a utilização dessas tecnologias em face das garantias processuais asseguradas ao acusado.

No levantamento realizado, foram identificados quatro julgados pertinentes à temática, sendo um oriundo do Tribunal de Justiça do Estado de Mato Grosso do Sul, um do Superior Tribunal de Justiça e dois do Supremo Tribunal Federal. As decisões analisadas envolvem a utilização da ferramenta de análise forense digital *Cellebrite*, empregada na extração e no exame de dados armazenados em dispositivos eletrônicos, em investigações relacionadas a crimes que não se restringem ao ambiente cibernético. Entre os casos encontrados, figuram processos relacionados aos delitos de homicídio e tráfico de drogas, os quais serão examinados nas subseções seguintes, considerando as particularidades de cada decisão e os fundamentos adotados pelos respectivos órgãos julgadores.

Embora a pesquisa tenha buscado decisões relacionadas ao emprego de ferramentas de inteligência artificial na investigação e persecução de crimes cibernéticos, verificou-se a existência de uma importante lacuna jurisprudencial sobre o tema. Para ampliar a abrangência do levantamento, foram utilizadas, como palavras-chave, as denominações de diferentes ferramentas empregadas na investigação e análise de evidências digitais, incluindo “Cellebrite”, “Peritus”, “Avilla Forensics”,

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VI, v.1 2025 | submissão: 20/12/2025 | aceito: 23/12/2025 | publicação: 26/12/2025

"NuDetective", "Watson Explorer", "Nuix Workstation" e "Autopsy Forensics". A busca resultou na localização de decisões relacionadas ao crime de armazenamento e compartilhamento de material contendo pornografia envolvendo crianças e adolescentes, previsto no artigo 241-A do Estatuto da Criança e do Adolescente (Brasil, 1990).

Entretanto, embora tais decisões apresentassem relação com a utilização de ferramentas tecnológicas na investigação de crimes praticados ou instrumentalizados por meios digitais, o objeto dos recursos analisados não se concentrava em eventual violação das garantias processuais do acusado decorrente do emprego dessas tecnologias. Em determinados casos, a controvérsia submetida ao Poder Judiciário não abrangia a validade ou os limites da utilização das ferramentas de inteligência artificial como meio de obtenção ou análise da prova. Em outros, o recurso sequer chegou a ter seu mérito apreciado, em razão de sua extinção por inadequação da via processual escolhida.

Dessa forma, o levantamento jurisprudencial evidencia uma limitada produção de decisões judiciais brasileiras que enfrentem, de maneira direta e específica, a compatibilidade entre o emprego de ferramentas tecnológicas de análise forense digital e as garantias processuais do acusado, no contexto dos crimes cibernéticos. Essa constatação reforça a necessidade de examinar os precedentes encontrados, ainda que relacionados a crimes diversos, uma vez que permitem identificar os critérios que vêm sendo considerados pelo Poder Judiciário brasileiro quanto à autorização judicial, ao acesso aos dados, à possibilidade de fiscalização pela defesa e à preservação das garantias fundamentais durante a utilização dessas tecnologias.

CONCLUSÃO

A incorporação da inteligência artificial e de ferramentas de análise forense digital à persecução penal representa uma transformação relevante na atividade investigativa contemporânea. A capacidade de processar grandes volumes de informações, recuperar dados, identificar padrões e auxiliar na interpretação de elementos digitais oferece ao Estado instrumentos importantes para o esclarecimento de infrações penais. Entretanto, a eficiência proporcionada pela tecnologia não pode ser compreendida como fundamento suficiente para afastar as garantias constitucionais que limitam o exercício do poder punitivo.

A análise desenvolvida ao longo deste estudo demonstra que a utilização de tecnologias aplicadas à investigação criminal deve permanecer subordinada aos princípios constitucionais e processuais que estruturam o processo penal brasileiro. O devido processo legal, o contraditório, a ampla defesa, a presunção de inocência, a proteção da intimidade e da vida privada e a inadmissibilidade das provas obtidas por meios ilícitos constituem parâmetros indispensáveis para avaliar a legitimidade dos procedimentos tecnológicos empregados na persecução penal.

No âmbito da prova digital, a preservação da integridade e da autenticidade dos dados assume

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VI, v.1 2025 | submissão: 20/12/2025 | aceito: 23/12/2025 | publicação: 26/12/2025

importância ainda maior. A possibilidade de alteração, duplicação ou eliminação de informações digitais exige procedimentos adequados de coleta, armazenamento, análise e documentação. Nesse contexto, a cadeia de custódia desempenha papel fundamental, pois permite acompanhar a trajetória do elemento probatório e estabelecer mecanismos de controle sobre sua integridade. A utilização de ferramentas tecnológicas sofisticadas, portanto, não elimina a necessidade de procedimentos rigorosos de preservação da prova.

A análise jurisprudencial realizada também permitiu constatar que a produção de precedentes brasileiros voltados à utilização de inteligência artificial na persecução de crimes cibernéticos ainda é limitada. Os julgados identificados concentram-se na utilização da ferramenta forense digital Cellebrite em investigações relacionadas a crimes como homicídio e tráfico de drogas. Nos casos examinados, os tribunais consideraram relevantes fatores como a existência de autorização judicial, a possibilidade de acesso aos elementos probatórios pela defesa e a observância dos mecanismos processuais destinados à proteção dos direitos fundamentais.

Por outro lado, a pesquisa revelou uma lacuna significativa quando se busca jurisprudência na qual a questão central seja a compatibilidade entre ferramentas de inteligência artificial e garantias processuais no contexto dos crimes cibernéticos. Embora tenham sido localizadas decisões envolvendo ferramentas tecnológicas e investigações relacionadas ao artigo 241-A do Estatuto da Criança e do Adolescente, os recursos examinados não apresentavam como objeto principal a discussão sobre violação das garantias do acusado decorrente da utilização dessas tecnologias, ou não tiveram seu mérito analisado em razão de questões processuais.

Essa ausência de jurisprudência consolidada demonstra que o desenvolvimento tecnológico está ocorrendo em ritmo superior ao amadurecimento da discussão judicial sobre seus limites. A inexistência de quantidade significativa de precedentes específicos, contudo, não significa ausência de parâmetros jurídicos. As garantias constitucionais e as regras processuais vigentes permanecem aplicáveis às novas formas de investigação, ainda que determinadas tecnologias não tenham sido previstas pelo legislador no momento de sua criação.

Nesse sentido, a autorização judicial, quando exigida pela natureza da medida, constitui importante instrumento de controle sobre a utilização das tecnologias de investigação. Da mesma forma, a possibilidade de fiscalização pela defesa deve ser preservada, permitindo que os elementos obtidos por sistemas tecnológicos sejam conhecidos, analisados e questionados. A transparência do procedimento é relevante quando a tecnologia utilizada apresenta elevado grau de complexidade ou emprega mecanismos automatizados de análise.

Conclui-se, portanto, que a inteligência artificial pode representar importante instrumento de modernização da persecução penal, mas sua utilização deve ocorrer dentro de parâmetros jurídicos estabelecidos e submetida a mecanismos efetivos de controle. A tecnologia não deve substituir as garantias processuais, tampouco transformar a busca pela eficiência investigativa em justificativa para

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VI, v.1 2025 | submissão: 20/12/2025 | aceito: 23/12/2025 | publicação: 26/12/2025

relativização indiscriminada dos direitos fundamentais.

O desafio colocado ao Direito consiste em estabelecer um equilíbrio entre a inovação tecnológica e a proteção das liberdades individuais. O enfrentamento da criminalidade contemporânea exige instrumentos compatíveis com a realidade digital, mas a modernização da investigação não pode significar retrocesso nas garantias conquistadas pelo Estado Democrático de Direito. Nesse cenário, o desenvolvimento de critérios jurisprudenciais mais específicos e de regulamentação adequada mostra-se necessário para conferir segurança jurídica à utilização da inteligência artificial na persecução penal, assegurando a efetividade da investigação e a proteção dos direitos fundamentais do acusado.

REFERÊNCIAS

ALMEIDA, Ivo Filipe de. A prova digital. 2014. Dissertação de Mestrado. Universidade Autônoma de Lisboa. Lisboa, 2014.

ALVES, Italo Miqueias da Silva. A Insurgência Tecnológica na Relação Probatória Processual Penal: A problemática do uso da prova digital no processo penal brasileiro no contexto da ausência legislativa regulatória. Jornal Tribuna. 2022. Disponível em: https://jornaltribuna.com.br/wp-content/uploads/2022/10/A-INSURGENCIA-TECNOLOGICA-NA-RELACAO-PROBATORIA-PROCESSUAL-PENAL-Italo-Miqueias-da-Silva-Alves.pdf.

BADARÓ, Gustavo Henrique. Processo Penal. 9ª Edição. São Paulo. Revista dos Tribunais. Thomson Reuters Brasil, 2021.

BRANCO, José Ricardo Marques. Prova digital. Os meios de obtenção de prova digital e a restrição de direitos do arguido. Dissertação de Mestrado. Universidade de Coimbra, 2021. Disponível em: https://estudogeral.uc.pt/handle/10316/94718.

BRASIL. Lei nº 11.690, de 09 de junho de 2008. Altera dispositivos do Decreto-Lei nº 3.689, de 3 de outubro de 1941 – Código de Processo Penal, relativos à prova, e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11690.htm.

BRASIL. Câmara dos Deputados. Projeto de Lei nº 4939, de 15 de outubro de 2020. Dispõe sobre as diretrizes do direito da Tecnologia da Informação e as normas de obtenção e admissibilidade de provas digitais na investigação e no processo, além de outras providências. Brasília, 2020.

BRASIL. LEI Nº 13.105, DE 16 DE MARÇO DE 2015. Código de Processo Civil. Brasília, 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm.

CASEY, Eoghan. Digital Evidence and Computer Crime. Forensic Science, computers and the internet. Third Edition. San Diego, Califórnia. Elsevier Academic Press, 2011, p. 07.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VI, v.1 2025 | submissão: 20/12/2025 | aceito: 23/12/2025 | publicação: 26/12/2025

FARAH, Camel André de Godoy. Terrorismo, Narcotráfico, Organizações Criminosas e Crimes Digitais. Palhoça: Unisul Virtual, 2019.

FERREIRA, Caio Porto. Hacking e infiltração policiais em resposta ao uso de criptografia por organizações criminosas. Revista Brasileira de Ciências Policiais, v. 12, n. 5, p. 19-48, 2021. Disponível em: https://periodicos.pf.gov.br/index.php/RBCP/article/view/837.

FIDALGO, Sônia. A utilização de inteligência artificial na obtenção de prova digital em processo penal. Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra, p. 07-08, dez. 2022.

FONTENELE, Diego Lemos; HOMSI, Larissa Cavalcante; GONÇALVES, Rafael Mota. A Prova Digital no Direito Processual Brasileiro. Revista Acadêmica da Escola Superior do Ministério Público do Ceará, v. 13, n. 1, p. 11–34, 2021. Disponível em:

FREITAS, Elison de Araújo; SILVA, Pedro Henrique Aguiar; SOUZA, Márcio Cabral de. Crimes Cibernéticos: Desafios da Investigação e Preservação das Provas. Facit Business and Technology Journal, v. 1, n. 44, 2023.

LANTYER, Victor Habib. Direito Digital e Inovação. Salvador. Editora Navida, 2023.

LIMA, Renato Brasileiro de. Código de Processo Penal Comentado. 2ª Edição. Salvador. Juspodivm, 2017.

MINTO, Andressa Olmedo. A Prova Digital no Processo Penal. 1ª Edição. São Paulo. LiberArs, 2021.

PETEAN, Fabiano Augusto; CASTILHO, Bruno Cardenal. A inadmissibilidade de provas ilícitas no processo penal brasileiro: Uma análise sobe a perspectiva de Robert Alexy. Revista de Direito, v. 11, n. 02, p. 127-145, 2020. Disponível em: https://periodicos.ufv.br/revistadir/article/view/8815

PRADO, Geraldo. Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital. Revista Consultor Jurídico, v. 26, 2021, p. 01.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VI, v.1 2025 | submissão: 20/12/2025 | aceito: 23/12/2025 | publicação: 26/12/2025

STOYKOVA, Radina. Digital Evidence: Unaddressed threats to fairness and the presumption of innocence. Computer Law & Security Review, v. 42, set. 2021. Disponível em: https://www.sciencedirect.com/science/article/pii/S0267364921000480.

STOYKOVA, Radina. The Presumption of Innocence as a Source for Universal Rules on Digital Evidence: The guiding principle for digital forensics in producing digital evidence for criminal investigations. Computer Law Review International, v. 22, n. 3, p. 74-82, 2021. Disponível em: https://pure.rug.nl/ws/portalfiles/portal/177956094/10.9785_cri_2021_220303.pdf.

SUPERIOR TRIBUNAL DE JUSTIÇA. AGRAVO EM RECURSO ESPECIAL Nº 2083614/SC (2022/0066832-9). Ministro Relator Reynaldo Soares da Fonseca. Brasília, 12 fev. 2023.

SUPREMO TRIBUNAL FEDERAL. RECLAMAÇÃO 49.369 RS. Min. Relator Ricardo Lewandowski. Brasília, 21 set. 2021.

VAZ, Denise Provasi. Provas Digitais no Processo Penal: Formulação do conceito, definição das características e sistematização do procedimento probatório. 2012. Tese (Doutorado). Faculdade de Direito da Universidade de São Paulo, São Paulo, 2012, p. 63.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.