DIREITO & TI
ISSN 2447-1097
WWW.DIREITOETI.COM.BR

Persecução penal digital: a prova na era da informação

Digital criminal prosecution: evidence in the information age

Marcelo Mendes Arigony[1]
Letícia Thomasi Jahnke Botton[2]
Ana Luiza Ortiz Arigony[3]

Recebido em: 16.10.2024
Aprovado em: 28.01.2025

RESUMO

Este artigo explora a investigação criminal no ambiente digital, com base em um caso de homicídio ocorrido em Santa Maria (RS) em 2023. O problema investigado refere-se ao papel das provas digitais na apuração de crimes complexos, como o homicídio, e a eficácia das ferramentas tecnológicas utilizadas para coleta e análise dessas evidências. O objetivo principal é analisar o impacto das provas digitais na resolução de crimes e propor melhorias para a investigação criminal no contexto digital. A justificativa do estudo reside na crescente importância das provas digitais no processo penal e no aumento dos crimes cibernéticos, demandando modernização nas práticas investigativas. A metodologia adotada é qualitativa, com revisão bibliográfica e análise de um estudo de caso, baseado em fontes primárias. A pesquisa demonstra a relevância das provas digitais na investigação criminal e sugere estratégias de aprimoramento para a atuação policial. O artigo aborda a revisão da literatura sobre prova digital no processo penal, a metodologia utilizada, a análise do caso concreto e a discussão dos resultados. Os resultados indicam que as ferramentas tecnológicas foram cruciais para a coleta de provas e identificação dos autores, reforçando a importância dessas tecnologias no processo investigativo.

Palavras-chave: homicídio; investigação criminal; prova digital; tecnologia.

ABSTRACT

This article explores criminal investigation in the digital environment, based on a homicide case that occurred in Santa Maria (RS) in 2023. The research problem concerns the role of digital evidence in solving complex crimes, such as homicide, and the effectiveness of technological tools used for collecting and analyzing such evidence. The main objective is to analyze the impact of digital evidence on crime resolution and

1 Doutor em Administração PPGA/UFSM com estágio pós-doutoral pela Universidade Luterana do Brasil – ULBRA. E-mail: marceloarigony@hotmail.com. Lattes: http://lattes.cnpq.br/9546846909596899
2 Doutora em Direito, com estágio de pós-doutorado pela Universidade de Salamanca. E-mail: leticiatjbotton@gmail.com. Lattes: http://lattes.cnpq.br/7443349048300506
3 Mestranda em Engenharia de Produção pela Universidade Federal de Santa Maria (UFSM). E-mail: anaarigony@gmail.com http://lattes.cnpq.br/7224095637142398

propose improvements for criminal investigations in the digital context. The study is justified by the growing importance of digital evidence in criminal proceedings and the increase in cybercrimes, which demand modernization in investigative practices. The methodology adopted is qualitative, involving a literature review and a case study analysis based on primary sources. The research demonstrates the relevance of digital evidence in criminal investigations and suggests strategies for enhancing police work. The article covers a literature review on digital evidence in criminal proceedings, the methodology used, the analysis of the specific case, and the discussion of the results. The findings indicate that technological tools were crucial for evidence collection and suspect identification, reinforcing the importance of these technologies in investigative processes.

Keywords: homicide; criminal investigation; digital evidence; technology.

1 INTRODUÇÃO

Vivemos em uma sociedade profundamente impactada pela revolução técnico-científica, que transformou o paradigma de interação social, migrando de um modelo analógico para um contexto predominantemente digital. Esse novo cenário exige adaptações, especialmente no campo das investigações criminais. Este trabalho examina o uso de novos instrumentos investigativos, adequados ao atual contexto da sociedade digital, no qual as provas eletrônicas e o uso de tecnologias são essenciais para elucidar crimes graves, como o homicídio.

O artigo explora a prova penal, trazendo como pano de fundo a investigação criminal no ambiente digital, a partir de um caso de homicídio ocorrido em Santa Maria (RS) no ano de 2023. Nesse contexto, as ferramentas tecnológicas desempenharam um papel crucial na descoberta e análise de evidências digitais, permitindo a apuração do crime e a identificação dos autores.

O problema central é entender a importância da prova digital no atual momento, e como as ferramentas tecnológicas podem ser aplicadas na investigação e resolução de crimes em que as evidências são coletadas em ambientes virtuais, como redes sociais. Diante disso, questiona-se: de que forma o uso de ferramentas digitais pode contribuir para a resolução de crimes no atual contexto social?

Os objetivos do estudo incluem realizar uma breve revisão bibliográfica sobre a prova no processo penal, abordando sua inserção no contexto digital; apresentar o estudo

de um caso de homicídio ocorrido na cidade de Santa Maria (RS) em 2023, que serviu de base para a análise; analisar e identificar as ferramentas digitais utilizadas na investigação criminal; e avaliar o impacto da prova digital na resolução de crimes, propondo estratégias para o aprimoramento das investigações criminais no ambiente digital.

O estudo é relevante para o campo jurídico, pois trata da crescente utilização de provas digitais no processo penal, em um cenário de evolução tecnológica e aumento dos crimes cibernéticos. Analisa a adequação dessas provas às garantias constitucionais, colaborando para o debate sobre a modernização das práticas jurídicas. Dessa forma, o trabalho contribui para o aprimoramento da atuação jurídica em processos que envolvem o ambiente digital e as novas exigências legais.

O estudo ainda se justifica pela contribuição para entender o impacto dos crimes digitais, como os praticados por meio de falsas identidades, no cotidiano das pessoas. Ele explora a utilização de ferramentas tecnológicas para investigar crimes graves, como homicídios. A pesquisa também pretende fortalecer as políticas públicas de segurança, ao trazer luz à necessidade de proteger direitos fundamentais, notadamente relacionados à privacidade de dados pessoais sensíveis.

No campo policial, o trabalho mostra relevância por investigar o uso de novas tecnologias na apuração de crimes. A pesquisa é essencial para o aprimoramento das atividades investigativas, ajudando a modernizar práticas diante dos desafios da era digital. Inserido na linha de pesquisa do doutorado em Políticas Públicas, Desenvolvimento Humano e Sociedade, o estudo visa aprimorar as investigações criminais e fortalecer as políticas públicas para enfrentar crimes cibernéticos.

O trabalho adota uma abordagem qualitativa, centrada na análise de um estudo de caso concreto. A metodologia busca compreender o papel das tecnologias digitais nas investigações criminais e como essas ferramentas podem contribuir para a resolução de crimes complexos. Inicialmente será realizada pesquisa bibliográfica sobre a prova no processo penal, focando nas provas digitais e nos crimes cibernéticos, a partir de obras jurídicas, artigos científicos e jurisprudência relevantes.

Em seguida será analisado um caso de homicídio de 2023 em Santa Maria, com base em fontes primárias, como relatórios de investigação, laudos periciais e outros

documentos do inquérito policial, identificando as ferramentas digitais utilizadas, como busca de dados de redes sociais, análise forense de dispositivos eletrônicos e rastreamento digital.

Destaque-se que no decorrer da elaboração do estudo será utilizada a ferramenta de inteligência artificial desenvolvida pela OpenAI, como auxiliar na revisão textual, busca de referências acadêmicas e sugestões para aprimoramento. A ferramenta atua como um suporte na verificação da fluidez e coesão do conteúdo, sendo ao final totalmente revisado pelo autor, assegurando que a redação atenda aos padrões de originalidade e ética acadêmica.

Na análise e discussão dos resultados, serão examinadas algumas ferramentas digitais utilizadas no caso base, e sua importância para a elucidação do crime. A análise está focada na maneira como as provas digitais foram coletadas e empregadas para identificar os autores do crime, além de discutir sua validade e impacto no processo investigativo. A partir disso, foram evidenciados os desafios e as oportunidades que essas tecnologias trazem para o aprimoramento das investigações criminais, especialmente no ambiente digital.

A estrutura do artigo segue a partir da Introdução, que apresenta o tema, o problema de pesquisa, os objetivos, a justificativa e a metodologia. A revisão bibliográfica inicia sobre a prova no processo penal, abordando também crimes cibernéticos e o uso de provas digitais no contexto jurídico. A Metodologia detalha o estudo de caso e as ferramentas digitais utilizadas na investigação.

Por fim, haverá análise do impacto das provas digitais na resolução de crimes, destacando a importância das tecnologias no processo investigativo. Também serão discutidos os desafios éticos e jurídicos que surgem com o uso dessas inovações, reforçando a necessidade de modernizar as práticas investigativas e garantir a proteção dos direitos fundamentais, como a privacidade e a presunção de inocência.

2 PROVA NO PROCESSO PENAL

No campo do direito processual penal, a prova se configura como o principal instrumento para a busca da verdade real em relação aos fatos que envolvem um crime. O processo penal visa assegurar a correta aplicação da justiça, garantindo que as decisões judiciais sejam fundamentadas em elementos concretos, resultantes da produção probatória. Segundo Tourinho Filho, a prova é definida como o meio pelo qual se verifica a existência ou inexistência de um fato que é relevante para o processo, seja em benefício ou em desfavor do réu (Tourinho Filho, 2023, p. 502).

A produção de provas tem como objetivo central assegurar a aplicação justa da lei, embasada no princípio da verdade real, que busca esclarecer os eventos tal como realmente ocorreram, ao invés de se restringir à forma como foram apresentados pelas partes. Para Capez (2023, p. 83-91)., a prova no processo penal é fundamental para formar o convencimento do juiz, sendo este o destinatário final do material probatório coletado no curso da investigação.

Ademais, a prova desempenha um papel essencial no equilíbrio entre a acusação e a defesa, sustentando os princípios do contraditório e da ampla defesa, pilares do devido processo legal. A coleta e a produção de provas devem ocorrer de forma imparcial, respeitando os direitos fundamentais do acusado e prevenindo qualquer forma de contaminação probatória, conforme preconizado no artigo 5º, inciso LVI, da Constituição Federal. (Brasil, 1988).

No âmbito jurídico-penal, a prova constitui mecanismo primário para buscar a verdade real dos fatos em um processo, desempenhando um papel vital na resolução de questões relacionadas à prática de crimes. Guilherme de Souza Nucci caracteriza a prova como "todo meio utilizado para demonstrar a veracidade ou a falsidade de um fato relevante para a resolução do processo" (Nucci, 2020, p.684). Tal definição reforça a importância da prova na formação do convencimento do juiz, que é o destinatário final da atividade probatória.

As provas no processo penal podem ser classificadas de diversas maneiras. Existem as provas pessoais, como testemunhos e confissões, e as provas materiais, que

incluem perícias e documentos. Além disso, é importante distinguir entre provas nominadas, que estão expressamente previstas na legislação, e provas inominadas, que são admitidas com base no princípio da verdade real, desde que respeitados os limites legais (Lopes Júnior, 2020, p. 459). A liberdade probatória é a regra no processo penal, mas encontra restrições, como em relação à vedação do uso de provas ilícitas.

A Constituição Federal, em seu artigo 5º, inciso LVI, e o Código de Processo Penal, em seu artigo 157, estabelecem que são inadmissíveis as provas obtidas por meios ilícitos. Provas ilícitas são aquelas obtidas em violação a normas constitucionais ou legais, como confissões extraídas sob tortura ou a invasão de privacidade sem a devida autorização judicial (Avena, 2020, p.949). Esse princípio é crucial para assegurar que o processo penal respeite as garantias constitucionais, mantendo a integridade do devido processo legal, do contraditório e da ampla defesa.

Além das classificações mencionadas, as provas no processo penal podem ser subdivididas em diretas e indiretas (ou indiciárias). As provas diretas são aquelas que estabelecem um vínculo imediato com o fato, como o testemunho de uma testemunha ocular, enquanto as provas indiretas, como indícios, permitem que o julgador chegue a uma conclusão por meio de uma sequência lógica que, embora não tenha relação direta com o fato principal, constrói um caminho de inferência (Lopes Júnior, 2020, p. 414).

Outra classificação relevante se relaciona ao meio de obtenção das provas. As provas nominadas são aquelas expressamente previstas na legislação, como a perícia técnica, conforme descrito nos artigos 158 a 250 do Código de Processo Penal. Já as provas inominadas não estão expressamente previstas na legislação, mas podem ser admitidas com base no princípio da verdade real, desde que respeitadas as normas processuais e constitucionais (Vasconcellos, 2018). Nesse sentido, o sistema penal brasileiro adota o livre convencimento motivado, permitindo ao juiz avaliar as provas, desde que respeitadas as garantias do contraditório e da ampla defesa.

Por último, há a distinção entre provas plenas e provas não plenas. As provas plenas são aquelas que, por si só, têm valor suficiente para fundamentar uma decisão judicial, como documentos que comprovam a materialidade do crime ou confissões que não apresentam vícios. Por outro lado, as provas não plenas requerem complementação

por outros elementos probatórios para formar um conjunto robusto que possa levar à condenação (Nucci, 2020; Avena, 2020). Esta classificação é fundamental para garantir a correta avaliação das provas no processo penal, assegurando que as condenações se baseiem em um conjunto probatório sólido e devidamente respaldado pela lei.

Além de ser meio de verificação dos fatos, a prova desempenha papel essencial na busca da verdade, um dos princípios fundamentais que regem o sistema penal. Embora a acusação tenha a responsabilidade de apresentar provas, o réu também tem o direito de produzir elementos probatórios que possam beneficiá-lo ou levar à sua absolvição. Esta interação entre as partes é vital, pois possibilita que tanto a acusação quanto a defesa apresentem suas evidências e argumentos, promovendo um julgamento mais justo e equilibrado (Avena, 2020).

Adicionalmente, a prova no processo penal não é meramente um meio de busca da verdade, mas um elemento que deve ser avaliado com um olhar crítico. O sistema penal precisa garantir que as provas sejam obtidas e avaliadas de forma a não comprometer os direitos fundamentais do acusado. Nesse contexto, a função da prova no processo penal transcende a mera busca da verdade, assumindo um papel essencial na proteção das garantias constitucionais. Assim, é imprescindível que apenas elementos probatórios obtidos de forma lícita e regular sejam considerados válidos para embasar decisões condenatórias.

A evolução da teoria da prova no processo penal reflete as transformações sociais e tecnológicas ao longo do tempo. Historicamente, as provas eram predominantemente físicas e testemunhais, baseadas na apresentação de evidências tangíveis e no testemunho de pessoas que vivenciaram os fatos. No âmbito social, é preciso compreender que “as novas tecnologias da informação não são simplesmente ferramentas a serem aplicadas, mas processos a serem desenvolvidos” (Castells, 1999, p.108).

Com o advento da era digital, a natureza das provas começou a se modificar, incorporando dados eletrônicos coletados de dispositivos como computadores e smartphones. Essa transição representa adaptação às novas realidades da criminalidade, e, também o reconhecimento da necessidade de incluir os novos tipos de provas no

sistema judicial, buscando uma verdade processual mais abrangente (Wendt; Rita da Costa; Barreto, 2023, p.55).

A admissibilidade da prova digital no ordenamento jurídico brasileiro é garantida pelo Código de Processo, que permite a utilização de diversos tipos de provas, incluindo as eletrônicas. O artigo 155 do Código estabelece que "a prova deve ser obtida por meios lícitos, sendo inadmissíveis as provas obtidas em desacordo com as normas legais". Isso abre espaço para que as provas digitais, desde que coletadas e apresentadas de acordo com os preceitos legais, sejam aceitas em juízo. Portanto, a prova digital não apenas amplia o arsenal probatório disponível, mas também exige que os operadores do direito estejam preparados para lidar com as complexidades e os desafios que surgem com essa nova forma de evidência.

A prova digital é uma ferramenta essencial nas investigações criminais, permitindo a coleta e análise de dados em um contexto em que a tecnologia permeia as relações sociais. Segundo Wendt, Rita da Costa e Barreto (2023, p.3), essa modalidade de prova não só facilita a elucidação de fatos, mas também exige que os operadores do direito estejam aptos a compreender as especificidades e complexidades envolvidas na manipulação de evidências eletrônicas.

A documentação adequada da cadeia de custódia e os protocolos de preservação são fundamentais para garantir a integridade e a admissibilidade das provas digitais em juízo, refletindo a necessidade de um conhecimento técnico profundo por parte dos profissionais do direito (Wendt; Rita da Costa; Barreto, 2023, p.204).

Os mesmos autores acima referidos informam que com o avanço das tecnologias, a prova digital se tornou uma forma inovadora de garantir a verdade processual, ao mesmo tempo em que demanda dos profissionais do direito uma atualização constante sobre as práticas e legislações relacionadas à sua utilização. A interseção entre direito e tecnologia continua a evoluir, fazendo com que a prova digital seja um campo em expansão que exige atenção especial para que suas potencialidades sejam plenamente aproveitadas sem comprometer os direitos fundamentais dos indivíduos.

O Código de Processo Penal (CPP), em seu art. 155, bem como Constituição Federal, em seu artigo 5º, inciso LVI, reforçam a inadmissibilidade de provas obtidas por

meios ilícitos, estabelecendo um pilar importante para a aceitação de provas digitais no sistema jurídico brasileiro. Adicionalmente, a Lei Geral de Proteção de Dados (LGPD, Lei nº 13.709/2018) e o Marco Civil da Internet (Lei nº 12.965/2014) desempenham papéis fundamentais na regulamentação da coleta e utilização de provas digitais, assegurando a privacidade e proteção dos dados pessoais.

3 CRIMES CIBERNÉTICOS E PROTEÇÃO DE DADOS

Os crimes cibernéticos são definidos como atividades ilícitas que ocorrem no ambiente digital, utilizando a tecnologia da informação como meio para a prática de delitos. Segundo Wendt, Rita da Costa e Barreto (2023, p.1), esses crimes abrangem uma variedade de infrações, desde fraudes eletrônicas até invasões de sistemas e roubo de dados pessoais. A principal distinção entre os crimes cibernéticos e os crimes tradicionais é o uso da tecnologia, o que impõe desafios únicos na investigação e persecução penal. A digitalização das infrações permite que criminosos operem além das fronteiras físicas, tornando a aplicação da lei e a cooperação internacional mais complexas.

Uma característica importante dos crimes cibernéticos é a evolução das formas de cometimento das infrações, que requer uma adaptação das legislações existentes para abordar as particularidades do ambiente digital. Leis como a Lei Carolina Dieckmann (Lei n.12.737/2012) e o Marco Civil da Internet (Lei n.12.965/2014) foram criadas para proteger a privacidade e segurança de dados pessoais no ambiente digital dos cidadãos e regulamentar o uso de tecnologia, reconhecendo as diversas formas de delitos que podem ocorrer online.

Os autores também ressaltam que, para lidar com os crimes cibernéticos, é crucial que os profissionais do direito compreendam as legislações pertinentes e as técnicas de investigação necessárias. A formação e a atualização constante dos operadores do direito são fundamentais para garantir uma resposta adequada a essas novas formas de criminalidade. Com a crescente utilização da internet, a necessidade de um quadro legal robusto e adaptável se torna ainda mais evidente, evidenciando a importância da

integração entre legislação e práticas investigativas eficazes (Wendt; Rita da Costa; Barreto, 2023).

Os crimes cibernéticos podem ser classificados em crimes próprios e impróprios. Os crimes próprios são aqueles em que o sistema informático é tanto o objeto quanto o meio do crime, ou seja, o delito não poderia ocorrer sem o uso do computador ou da rede. Exemplos incluem a invasão de dispositivos eletrônicos e a distribuição de malware, onde a violação das informações automatizadas é o cerne da infração. Já os crimes impróprios envolvem o uso da tecnologia como meio para realizar delitos tipificados que não dependem exclusivamente do ambiente digital, como a calúnia, injúria e difamação, onde o computador é utilizado apenas como um instrumento para a execução de atos que também poderiam ocorrer em ambientes físicos (Wendt; Rita da Costa; Barreto, 2023; Cunha, 2021).

A legislação brasileira busca acompanhar a evolução dos crimes cibernéticos, reconhecendo a importância de um quadro legal que trate das diversas formas de infração digital. Leis como a Lei Carolina Dieckmann (Lei nº 12.737/2012) e o Marco Civil da Internet (Lei nº 12.965/2014) estabelecem normas para a proteção dos cidadãos e a criminalização de práticas como a invasão de dispositivos eletrônicos (Brasil, 2012; Brasil, 2014).

Além disso, ao abordar crimes digitais e a utilização de perfis falsos para cometer crimes como o homicídio, é fundamental explorar a evolução das legislações relacionadas. A Lei Carolina Dieckmann (Lei nº 12.737/2012) foi um marco no combate aos crimes cibernéticos no Brasil, criminalizando a invasão de dispositivos eletrônicos e o acesso não autorizado a dados informáticos. A lei foi criada após um incidente envolvendo o vazamento de fotos privadas da atriz Carolina Dieckmann, e desde então passou a regular crimes digitais, trazendo maior segurança jurídica para as investigações. A utilização de perfis falsos, como no caso em estudo, pode ser considerada crime conforme essa lei, visto que muitas vezes envolve invasão de privacidade e apropriação indevida de dados (Brasil, 2012).

Ademais, as discussões legislativas sobre o uso de identidade falsa na internet têm ganhado relevância com o aumento dos crimes cometidos nesse ambiente. A Lei Geral

de Proteção de Dados (Lei nº 13.709/2018) é outra legislação importante que estabelece diretrizes claras sobre a coleta e o tratamento de dados pessoais, assegurando que o direito à privacidade dos cidadãos seja respeitado. Juntas, essas legislações reforçam a importância do uso legal e adequado de provas digitais, garantindo que as investigações envolvendo perfis falsos e outros delitos cibernéticos respeitem os direitos fundamentais e contribuam para a solução efetiva dos casos (Brasil, 2018).

A crescente incidência de crimes cibernéticos sublinha a importância da proteção de dados e da privacidade, temas que se tornaram centrais na era digital. A Lei Geral de Proteção de Dados (LGPD), sancionada em 2018, estabelece normas que visam garantir a proteção da privacidade dos cidadãos, assegurando que os dados pessoais sejam tratados de forma legal e transparente. A legislação requer que o tratamento de dados ocorra com o consentimento explícito e para finalidades específicas, refletindo uma clara preocupação com a autodeterminação informativa do indivíduo (Brasil, 2018).

Recentemente, o Supremo Tribunal Federal (STF) reconheceu a proteção de dados e a autodeterminação informativa como direitos fundamentais autônomos, destacando a necessidade de um arcabouço jurídico robusto que proteja esses direitos. Na decisão da ADIn 6393, a Corte abordou a importância de garantir que qualquer compartilhamento de dados pessoais respeite as normas de proteção e não comprometa a privacidade dos indivíduos (Brasil, 2024).

No voto proferido pelo ministro Gilmar Mendes na ADIn 6393, foi enfatizado que a proteção de dados pessoais está diretamente vinculada à dignidade da pessoa humana, sendo um direito fundamental que deve ser assegurado em qualquer contexto, independentemente do meio de coleta. Tal entendimento reforça a necessidade de um arcabouço legal que proteja os dados pessoais frente aos desafios impostos pela era digital, garantindo que a privacidade e os direitos individuais sejam resguardados (Migalhas, 2021). Nesse sentido, a Emenda Constitucional nº 115/2022, incluiu a proteção de dados como Direito Fundamental. “LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais (Incluído pela Emenda Constitucional nº 115, de 2022)”, o que reforça o acerto da decisão do STF.

No âmbito do Superior Tribunal de Justiça (STJ), a jurisprudência também tem se adaptado para lidar com questões de proteção de dados. No recente caso REsp 2.077.278-SP, o tribunal tratou do vazamento de dados bancários, onde a instituição financeira foi responsabilizada por não proteger adequadamente as informações pessoais dos consumidores. A decisão reforçou o dever das empresas de garantir a segurança dos dados que manipulam, conforme previsto no artigo 43 da LGPD, e destacou que a falha na proteção pode facilitar atividades criminosas (Brasil, 2023). Essa evolução na jurisprudência evidencia a crescente preocupação com a responsabilidade das empresas em relação ao tratamento e proteção de dados, promovendo um ambiente mais seguro para os cidadãos no contexto digital.

4 ESTUDO DE CASO DO HOMICÍDIO DE ROBIN

Inicialmente, é necessário destacar que, para preservar a privacidade e a identidade dos envolvidos, os nomes reais dos participantes foram substituídos por nomes fictícios, como Robin, Batman e Coringa. Essa abordagem visa garantir o respeito às partes envolvidas, ao tempo que permite discutir a relevância das provas e evidências digitais na elucidação do crime e seu papel na justiça penal. O uso de nomes fictícios assegura que a análise possa ser realizada sem comprometer a integridade do processo ou expor indevidamente os envolvidos no caso.

Além disso, é importante salientar que os detalhes mais específicos do caso não puderam ser abordados neste estudo, pois o processo ainda está em andamento, sem julgamento definitivo. Dessa forma, foram apresentados apenas dados genéricos para ilustrar a dinâmica da investigação. Para estudos futuros, após a conclusão do julgamento, é possível explorar as ferramentas digitais utilizadas, como o rastreamento de IP, as mensagens trocadas no WhatsApp, além dos áudios e outras evidências extraídas ao longo da investigação.

A investigação referente ao homicídio de Robin, ocorrido em abril de 2023, na cidade de Santa Maria (RS), revela a complexidade das interações entre tecnologia e criminalidade. Para além da tragédia individual, esse caso é também um exemplo da

crescente intersecção entre crimes e a utilização de tecnologias digitais. Robin foi executado por disparos de arma de fogo, à luz do dia, em via pública. As suspeitas iniciais recaíam sobre Batman, morador da Vila Xurupita e previamente investigado por homicídio qualificado, o que foi confirmado ao longo da investigação.

Câmeras de segurança capturaram a cena do crime, mostrando Batman chegando a cavalo e efetuando os disparos contra Robin. Durante o interrogatório perante a Autoridade Policial, Batman alegou que sua ação foi em legítima defesa, afirmando ter recebido ameaças de Robin por meio de um perfil na internet. As investigações subsequentes revelaram que o perfil responsável pelas ameaças foi criado por Coringa com a finalidade de induzir o homicídio.

No desenrolar da investigação, ficou claro que o autor do crime, Coringa, nutria medo profundo da vítima, Robin, que mantinha um relacionamento extraconjugal com a esposa do primeiro (Coringa). Temendo confrontar Robin diretamente, Coringa optou por uma estratégia elaborada para induzir sua morte. Ele criou uma página falsa no Facebook, usando a imagem de Robin, e a partir dessa página começou a ameaçar Batman e indivíduos perigosos da comunidade onde viviam. As ameaças, atribuídas falsamente a Robin, instigaram esses criminosos a acreditar que estavam sendo provocados por ele, levando Batman a executar o homicídio.

Esse caso revela uma autoria intelectual mediata, uma forma de indução ao crime que se diferencia pela sua complexidade e pela manipulação indireta das circunstâncias para atingir o objetivo final, um tipo de autoria rara e original no campo da criminologia, motivado por ciúme conjugal.

A análise das evidências digitais foi fundamental para esclarecer a dinâmica do crime. As conversas no WhatsApp entre Batman e Coringa, juntamente com registros de chamadas e mensagens, mostraram um planejamento detalhado que precedeu o homicídio. Tais dados, obtidos através de software forense, são exemplares da importância da prova digital na apuração de crimes complexos.

Como se infere da leitura de Thamay e Tamer (2020), as provas digitais, como e-mails e mensagens de texto, podem oferecer evidências precisas e frequentemente decisivas em processos judiciais, sendo crucial considerar sua obtenção e preservação

adequadas. Essa precisão é fundamental em um sistema onde as informações podem ser facilmente manipuladas.

Além disso, a legislação brasileira, como o Código de Processo Penal (CPP), estabelece que a prova deve ser coletada e tratada de maneira que preserve sua integridade. O artigo 158-A do CPP, reforçado pelo Pacote Anticrime (Lei n.13.964/2019), define a cadeia de custódia como o conjunto de procedimentos que garantem a autenticidade e integridade das provas digitais, desde sua coleta até a apresentação em juízo (Brasil, 2019).

A manutenção adequada dessa cadeia de custódia é vital, pois a falta de um registro rigoroso pode comprometer a admissibilidade das provas em tribunal. O Superior Tribunal de Justiça (STJ) tem enfatizado em suas decisões a importância da documentação cuidadosa durante todo o processo investigativo, alertando que falhas na cadeia de custódia podem levar à invalidação das provas (Brasil, 2023).

As provas digitais, como prints de conversas e registros de chamadas, foram cruciais para desmascarar a narrativa de Batman. A análise detalhada dos dados extraídos dos dispositivos móveis dos envolvidos, realizada por meio de técnicas forenses, permitiu não apenas a confirmação dos eventos, mas também a refutação das alegações de legítima defesa. A coleta e a preservação adequada dessas provas não apenas sustentaram a acusação, mas também ressaltaram o papel vital da tecnologia na investigação criminal moderna.

A conclusão da investigação resultou no indiciamento de Batman pelo homicídio qualificado de Robin e na responsabilização de Coringa por instigar a violência através do perfil falso. O inquérito foi encerrado com a recomendação de prisão preventiva de Batman, reforçando a necessidade de uma resposta rigorosa frente à gravidade dos atos cometidos. Essa investigação demonstra claramente como a prova digital se tornou um elemento central para a elucidação de crimes e a promoção da justiça no cenário contemporâneo.

A utilização de imagens de câmeras de segurança em investigações criminais é respaldada pela legislação brasileira, uma vez que essas imagens são consideradas provas digitais válidas. De acordo com o artigo 5º, inciso XII, da Constituição Federal, a proteção

à intimidade e à vida privada deve ser respeitada; no entanto, essa proteção não impede o uso de imagens capturadas em locais públicos, onde a expectativa de privacidade é reduzida (Brasil, 1988). O uso de câmeras em áreas públicas, como ruas e praças, é legal, permitindo que as gravações sejam empregadas como evidência em processos judiciais.

O artigo 158 do Código de Processo Penal (CPP) estabelece que as provas devem ser obtidas de forma lícita, e a prova ilícita é inadmissível. Assim, desde que a coleta das imagens siga essas diretrizes e não infrinja o direito à privacidade, elas podem ser utilizadas para esclarecer os fatos de um crime. Jurisprudências do Superior Tribunal de Justiça (STJ) confirma que a captação de imagens em espaço público é legal e pode ser utilizada para corroborar a narrativa da investigação, contribuindo para a formação do convencimento do juiz (Brasil, 2023; Kaspersky, 2024).

As imagens capturadas por câmeras de segurança desempenham um papel cada vez mais importante na coleta de evidências, auxiliando na cronologia de eventos, identificação de suspeitos e confirmação de testemunhos. Pesquisas indicam que essas imagens podem ser determinantes para a solução de crimes graves, como homicídios e roubos, com as gravações sendo fundamentais em até 65% das investigações (Ashby, 2023). O uso eficaz de tecnologias como o CCTV (Closed-Circuit Television) reforça a necessidade de uma abordagem investigativa moderna e integrada, assegurando que as provas digitais sejam preservadas e utilizadas adequadamente (Urban Institute, 2023).

Portanto, as imagens de câmeras de segurança desempenham um papel crucial na coleta de evidências, ajudando a estabelecer cronologias, identificar suspeitos e validar testemunhos. A análise rigorosa dessas imagens pode ser decisiva na resolução de crimes, evidenciando a eficácia das tecnologias digitais no sistema de justiça penal e reforçando a necessidade de uma abordagem moderna nas investigações (Migalhas, 2021).

A investigação teve êxito em identificar e coletar dados relativos ao momento da criação da conta falsa utilizada para ameaçar Robin, o que foi crucial para elucidar a dinâmica do crime. O acesso a informações sobre a criação da conta, incluindo o endereço IP utilizado para sua configuração, permitiu à equipe de investigação traçar um vínculo entre o autor da ameaça e o ato criminoso. O endereço IP (Internet Protocol) é uma peça-chave em investigações digitais, pois permite identificar a localização geográfica do

dispositivo usado para acessar a internet, facilitando o rastreamento do autor do crime (Wendt; Barreto; Rita Da Costa, 2023).

Para a obtenção dessas informações, foi necessária autorização judicial, conforme estipulado pelo artigo 5º da Constituição Federal e pela Lei Geral de Proteção de Dados (LGPD) (Brasil, 1988; 2018). O fornecimento de dados de conexão e o endereçamento de IP exigem rigorosos procedimentos legais para garantir a proteção dos direitos dos indivíduos e a legitimidade das provas. A legislação estabelece que a coleta de informações deve ser feita com base em ordem judicial, respeitando os princípios da necessidade e proporcionalidade, e a proteção aos direitos fundamentais deve orientar a obtenção e o uso das provas digitais no âmbito penal.

Assim, a análise meticulosa das provas digitais, aliada ao cumprimento das exigências legais, demonstrou-se essencial para o esclarecimento dos fatos e para a responsabilização dos envolvidos. As evidências coletadas não apenas corroboraram a narrativa da investigação, mas também destacaram a importância das tecnologias digitais no combate aos crimes. Com isso, a utilização de dados como o endereço IP se torna um instrumento valioso na identificação de criminosos e na reconstrução de eventos, reforçando a necessidade de abordagem integrada nas investigações (KASPERSKY, 2024).

A coleta de provas digitais, como conversas em aplicativos de mensagens, especialmente no WhatsApp, e registros de chamadas, é essencial nas investigações criminais contemporâneas, mas deve ser conduzida de acordo com rigorosos critérios legais para assegurar sua validade. Conforme estabelece o artigo 5º, inciso XII, da Constituição Federal, a proteção à intimidade e à vida privada é um direito fundamental, e qualquer intervenção na privacidade deve ser respaldada por uma justificativa legal adequada (BRASIL, 1988). Em situações que envolvem a coleta de provas digitais, a autorização judicial é imprescindível, garantindo que as ações investigativas não infrinjam direitos constitucionais.

A Lei Geral de Proteção de Dados (LGPD) também fornece diretrizes para o tratamento de dados pessoais, exigindo que a coleta ocorra com o consentimento do titular, salvo exceções definidas na legislação (Brasil, 2018). A jurisprudência brasileira,

especialmente as decisões do Superior Tribunal de Justiça (STJ), enfatiza que a interceptação de comunicações, como aquelas realizadas via WhatsApp, deve ser precedida de uma ordem judicial que justifique a medida, considerando sua necessidade e proporcionalidade (Brasil, 2023). A falta de autorização judicial adequada pode acarretar a nulidade das provas, comprometendo o processo investigativo.

Adicionalmente, a cadeia de custódia das provas digitais deve ser rigorosamente mantida, conforme estabelece o artigo 158-A do Código de Processo Penal (CPP), que define os procedimentos necessários para garantir a autenticidade e integridade das evidências (Brasil, 2019). A ausência de documentação e preservação adequada pode resultar na desconsideração das provas em juízo, conforme reforçado pelo STJ, que tem reiterado a importância de um controle rigoroso na manipulação de dados digitais (KASPERSKY, 2024). Portanto, a coleta de provas digitais, incluindo informações obtidas através do WhatsApp, deve ser realizada legalmente e seguir protocolos que garantam a legitimidade e eficácia das evidências no processo penal, assegurando a justiça e a proteção dos direitos individuais.

5 CONSIDERAÇÕES FINAIS

Este artigo apresentou uma investigação sobre caso inusitado, e bastante original no meio acadêmico, detalhando a relevância das provas digitais no contexto das investigações criminais, com foco específico no caso do homicídio de Robin na cidade de Santa Maria (RS). A análise revelou como a tecnologia tem desempenhado um papel transformador na coleta de evidências e na apuração de crimes, destacando a importância de ferramentas digitais como o WhatsApp e as câmeras de segurança na elucidação de casos complexos. Através da coleta meticulosa de dados e da análise das interações digitais, foi possível traçar conexões entre os suspeitos e os eventos que culminaram no crime, demonstrando a eficácia das provas digitais na justiça penal.

O estudo também enfatizou que, embora as provas digitais ofereçam uma nova perspectiva para a investigação criminal, sua coleta e utilização devem sempre respeitar os direitos fundamentais dos indivíduos, conforme estabelecido na legislação brasileira.

A necessidade de autorização judicial para a coleta de dados, bem como o cumprimento rigoroso da cadeia de custódia, foram elementos cruciais para garantir a legitimidade das provas apresentadas no processo. A conformidade com a Lei Geral de Proteção de Dados (LGPD) e com o Código de Processo Penal (CPP) assegura que as informações obtidas sejam admissíveis em juízo, protegendo os direitos à privacidade e à intimidade dos envolvidos.

Além disso, a evolução das tecnologias digitais exige uma constante atualização dos profissionais do direito para que possam lidar com as complexidades que surgem com a utilização de provas digitais. Os desafios da investigação cibernética, como a manipulação de dados e a transnacionalidade dos crimes, demandam uma adaptação das legislações e práticas jurídicas para que possam efetivamente enfrentar as novas formas de criminalidade. Portanto, a integração entre o direito e a tecnologia se mostra essencial para o desenvolvimento de um sistema jurídico que seja ágil, eficaz e justo.

Retomando o tema central deste estudo, que é a análise da importância das provas digitais nas investigações criminais, o problema de pesquisa delineou a necessidade de compreender como essas evidências podem ser utilizadas para esclarecer casos complexos, como o homicídio de Robin. Os objetivos propostos na introdução foram alcançados, pois realizamos uma revisão bibliográfica sobre a prova no processo penal, apresentamos o caso em questão, analisamos as ferramentas digitais utilizadas na investigação e avaliamos o impacto dessas provas na resolução do crime. Assim, este trabalho não apenas contribuiu para a compreensão da dinâmica do uso de provas digitais, mas também para o aprimoramento das práticas investigativas no contexto atual.

A introdução de tecnologias emergentes, como a inteligência artificial (IA), o aprendizado de máquina e o big data têm revolucionado o processo investigativo, permitindo análises mais rápidas e detalhadas. No entanto, essas inovações também levantam questões éticas e jurídicas. A IA, por exemplo, tem sido utilizada para identificar padrões de comportamento suspeito, mas o uso de algoritmos preditivos pode ferir o princípio da presunção de inocência, gerando perfis de risco que, por si só, não constituem prova material suficiente para justificar uma ação penal.

Em suma, a importância das provas digitais nas investigações criminais é indiscutível, pois elas não apenas oferecem uma nova abordagem para a coleta de evidências, mas também contribuem para a busca da verdade processual em um mundo cada vez mais informatizado. A intersecção entre tecnologia e direito deve ser explorada e aprimorada, garantindo que as investigações continuem a avançar em direção à justiça e à proteção dos direitos dos cidadãos.

Por fim, é essencial destacar o desafio de equilibrar a eficiência investigativa proporcionada pelas tecnologias digitais com a necessidade de preservar as garantias constitucionais. O princípio da proporcionalidade deve orientar todas as investigações, assegurando que a busca pela verdade real não se sobreponha aos direitos fundamentais, como a presunção de inocência e a proteção à privacidade.

O uso de provas digitais representa uma verdadeira revolução no campo da investigação criminal, mas requer uma abordagem cautelosa para que essas provas sejam admissíveis em juízo e obtenham a devida legitimação sem ferir as garantias processuais. A conformidade com a legislação vigente e o respeito aos direitos humanos são essenciais para assegurar que as inovações tecnológicas contribuam para a promoção da justiça, e não para a violação de liberdades civis.

Ressaltamos que, embora nossa análise tenha buscado destacar a relevância das provas digitais nas investigações criminais, o tema permanece em aberto, dada sua vastidão e complexidade, exigindo investigações mais profundas. A natureza inovadora das novas tecnologias demanda um esforço acadêmico contínuo para que possamos compreender plenamente suas implicações no processo penal.

É fundamental reconhecer nossa vulnerabilidade diante das tecnologias emergentes, que, embora tragam avanços significativos para a investigação criminal, também expõem fragilidades profundas. O cenário ainda é vastamente inexplorado, e essa incerteza nos deixa suscetíveis a diversas formas de ataques. No caso analisado, a criação de uma página falsa com a imagem da vítima ilustra como essas ferramentas podem ser utilizadas de maneira maliciosa, causando danos irreparáveis. O desafio que se impõe à justiça criminal é equilibrar o uso eficaz dessas tecnologias com a proteção dos direitos

fundamentais, navegando por esse território ainda desconhecido com prudência e responsabilidade.

Conforme Zygmunt Bauman (2000), estamos imersos em um período caracterizado pela modernidade líquida, onde as mudanças sociais, tecnológicas e econômicas desafiam nossas formas tradicionais de entender a realidade, que é marcada pela incerteza e fluidez.

Essa reflexão serve como um fechamento para nosso estudo, sublinhando a necessidade de avançarmos com investigações contínuas e abrangentes, evidenciando que a importância do tema não se limita ao campo jurídico, mas também se estende à formulação de estratégias que modernizem as práticas investigativas no cenário digital.

REFERÊNCIAS

ASHBY, M. P. J. The Value of CCTV for Criminal Investigation. **European Journal on Criminal Policy and Research**, 2023. Disponível em: https://www.researchgate.net/publication/316123456_The_Value_of_CCTV_for_Criminal_Investigation. Acesso em: 10 maio 2024.

AVENA, Norberto. **Processo Penal.** 12. ed. Rio de Janeiro: Forense, 2020.

BAUMAN, Zygmunt. **Liquid modernity.** Cambridge: Polity Press, 2000.

BRASIL. **Constituição Federal.** Brasília: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 17 mar. 2024.

BRASIL. Código de Processo Penal – **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Rio de Janeiro, RJ, 13 out. 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689.htmAcesso em: 07 jul. 2024.

BRASIL. **Decreto nº 11.491, de 12 de abril de 2023**. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Brasília, DF, 12 abr. 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/Decreto/D11491.htm. Acesso em: 05 jul. 2024.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de condutas praticadas contra dispositivos informáticos. Brasília, DF, 03 dez. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2012/l12737.htm. Acesso em: 11 maio 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Marco Civil da Internet. Brasília, DF, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2014-2018/2014/lei/L12965.htm. Acesso em: 27 jul. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2018-2022/2018/lei/L13709.htm. Acesso em: 10 maio 2024.

BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019**. Altera o Código Penal e o Código de Processo Penal. Brasília, DF, 24 dez. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm. Acesso em: 05 jul. 2024.

BRASIL. Superior Tribunal de Justiça. STJ. **Informativo de Jurisprudência n. 791**. 18 de outubro de 2023. Disponível em: https://processo.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisarumaedicao&livre=%270791%27.cod.#:~:text=791-,Informativo%20de%20Jurisprud%C3%AAncia%20n.,patrim%C3%B4nio%20deixado%20%C3%A0%20herdeira%20incapaz. Acesso em: 13 maio 2024.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade n° 6393**. Disponível em: https://www.stf.jus.br. Acesso em: 02 maio 2024.

CAPEZ, Fernando. **Curso de processo penal.** 30. ed. São Paulo: Saraiva, 2023.

CASTELLS, Manuel. **A sociedade em rede**. 2. ed. São Paulo: Paz e Terra, 1999.

CUNHA, Robson. **Crimes cibernéticos e o direito penal**. Rio de Janeiro: Forense, 2021.

KASPERSKY. **What is cybercrime and how to protect yourself?** Disponível em: https://www.kaspersky.com. Acesso em: 17 ago. 2024.

LOPES JÚNIOR, Aury. **Direito processual penal.** 10. ed. São Paulo: Saraiva, 2020.

MIGALHAS. **Decisão histórica:** STF reconhece direito autônomo à proteção de dados pessoais. Disponível em: https://www.migalhas.com.br. Acesso em: 19 mar. 2024.

MIGALHAS. **O crescimento do uso de provas digitais no sistema judicial brasileiro.** Disponível em: https://www.migalhas.com.br. Acesso em: 08 maio 2024.

NUCCI, Guilherme de Souza. **Código de processo penal comentado**. 18. ed. São Paulo: Editora Revista dos Tribunais, 2020.

TOURINHO FILHO, Fernando da Costa. **Processo penal.** 38. ed. São Paulo: Saraiva, 2023.

THAMAY, Rennan; TAMER, Maurício. **Provas no Direito Digital**: conceito da prova digital, procedimentos e provas digitais em espécie. São Paulo: Editora Revista dos Tribunais, 2020.

URBAN INSTITUTE. **How surveillance cameras can help prevent and solve crime.** Disponível em: https://www.urban.org. Acesso em: 10 jun. 2024.

VASCONCELLOS, Vinicius Gomes de. **A prova no processo penal**: a importância da valoração do lastro probatório e de seu controle por meio recursal. Revista Eletrônica do Curso de Direito da UFSM, Santa Maria, RS, v. 13, n. 2, p. 695-721, ago. 2018. ISSN 1981-3694. Disponível em: https://periodicos.ufsm.br/revistadireito/article/view/30012. Acesso em: 01.dez.2024. doi: http://dx.doi.org/10.5902/1981369430012.

WENDT, Emerson; RITA DA COSTA, Cristiano; BARRETO, Alberto. **Direito e tecnologia:** a nova era das provas digitais. São Paulo: Editora Saraiva, 2023.