FACULDADE EVANGÉLICA DE GOIANÉSIA
CURSO DE GRADUAÇÃO EM DIREITO

CADEIA DE CUSTÓDIA DA PROVA DIGITAL: MEIOS E LICITUDES DA PROVA DIGITAL PARA SUA ADMISSÃO NO PROCESSO PENAL

DOUGLAS OLIVEIRA SILVA
KELLITON CÉSAR DA SILVA

Goianésia/GO
2023

DOUGLAS OLIVEIRA SILVA
KELLITON CÉSAR DA SILVA

CADEIA DE CUSTÓDIA DA PROVA DIGITAL: MEIOS E LICITUDES DA PROVA DIGITAL PARA SUA ADMISSÃO NO PROCESSO PENAL

Trabalho de Conclusão de Curso apresentado à Faculdade Evangélica de Goianésia (FACEG), em nível de bacharel, como requisito parcial para obtenção do título de Bacharel em Direito.

Orientadora: Profa. Esp. Sara Moraes Vieira.

Goianésia/GO
2023

FOLHA DE APROVAÇÃO

CADEIA DE CUSTÓDIA DA PROVA DIGITAL: MEIOS E LICITUDES DA PROVA DIGITAL PARA SUA ADMISSÃO NO PROCESSO PENAL

Este Artigo Científico foi julgado adequado para a obtenção do título de Bacharel em Direito e aprovado em sua forma final pela banca examinadora da Faculdade Evangélica de Goianésia/GO- FACEG

Aprovada em, 11 de dezembro de 2023.

Nota Final__75___

Banca Examinadora

Prof.ª .....
Profa. Dra Sara Moraes Vieira.

Prof. .....

Jean Carlos Moura Mota

Prof. .....

Luana de Miranda Santos

CADEIA DE CUSTÓDIA DA PROVA DIGITAL: MEIOS E LICITUDES DA PROVA DIGITAL PARA SUA ADMISSÃO NO PROCESSO PENAL

DIGITAL EVIDENCE CHAIN OF CUSTODY: MEANS AND LAWSUIT OF DIGITAL EVIDENCE FOR ADMISSION IN THE CRIMINAL PROCESS

DOUGLAS OLIVEIRA SILVA[1]
KELLITON CÉSAR DA SILVA[1]
MAISA FRANÇA TEIXEIRA[2]

[1]*Discente do curso de Direito da Faculdade Evangélica de Goianésia- e-mail: do7073145@gmail.com*

[2]*Docente do curso de Direito da Faculdade Evangélica de Goianésia- e-mail: DIREITOTCCFINAL@GMAIL.COM*

RESUMO: A presente pesquisa, intitulada cadeia de custódia da prova digital: meios e licitudes da prova digital para sua admissão no processo penal, traz à tona uma discussão a respeito da evolução da tecnologia, o conceito de cadeia de custódia subsídios da Lei Anticrime, a investigação forense para o tratamento das evidências digitais e os tipos de crimes virtuais, com destaque para o caso da atriz Carolina Dieckmann. A escolha deste tema justifica-se pela grande quantidade de notícias diárias de pessoas que sofrem com crimes virtuais, tornando-se uma realidade cotidiana, onde buscar por proteção legal é de extrema importância. Diante disso, o objetivo geral deste estudo foi analisar o emprego da cadeia de custódia da prova digital e sua licitude, como meio de verificar quais os mecanismos utilizados para garantir a confiabilidade das provas digitais no processo penal. Já os objetivos específicos foram compreendidos por: identificar quais as leis e normas que garantem a aplicabilidade da cadeia de custódia da prova digital; descrever quais os meios para a admissão da prova digital no processo penal; verificar qual a relevância e o peso da prova digital no esclarecimento de crimes; avaliar a importância da prova digital nos crimes da contemporaneidade. Como metodologia de estudo, foi realizada uma análise de produções através da pesquisa bibliográfica via internet. Verificou-se a necessidade de continuarem sendo levantadas pautas de discussões e combate aos crimes virtuais, apresentando argumentos que comprovem a necessidade da admissão da cadeia de custódia da prova digital no processo penal.

PALAVRAS-CHAVE: Cadeia de custódia. Prova Digital. Processo Penal.

ABSTRACT: This research, entitled chain of custody of digital evidence: means and legalities of digital evidence for its admission in criminal proceedings, brings up a discussion about the evolution of technology, the concept of chain of custody, subsidies from the Anti-Crime Law, forensic investigation for the treatment of digital evidence and the types of virtual crimes, with emphasis on the case of actress Carolina Dieckmann. The choice of this topic is justified by the large number of daily reports of people suffering from cybercrime, making it a daily reality, where seeking legal protection is extremely important. Therefore, the general objective of this study was to analyze the use of the chain of custody of digital evidence and its legality, as a means of verifying which mechanisms are used to guarantee the reliability of digital evidence in criminal proceedings. The specific objectives were: to identify which laws and regulations guarantee the applicability of the chain of custody of digital evidence; to describe the means of admitting digital evidence into criminal proceedings; to verify the relevance and weight of digital evidence in clarifying crimes; and to assess the importance of digital evidence in contemporary crimes. As a study methodology, an analysis of productions was carried out through bibliographic research via the internet. It was found that there is a need to continue discussing and combating virtual crimes, presenting arguments that prove the need to admit the chain of custody of digital evidence in criminal proceedings.

KEYWORDS: Chain of custody. Digital Evidence. Criminal Procedure.

INTRODUÇÃO

A teoria da prova digital refere-se aos princípios e métodos utilizados na coleta, preservação, análise e apresentação de evidências digitais em processos judiciais ou investigações. Com o aumento da utilização de tecnologias da informação e comunicação, a prova digital tornou-se uma parte essencial de muitos casos legais (Badaró, 2021).

A cadeia de custódia refere-se ao registro documentado do controle e manipulação de evidências ao longo do tempo. Isso é fundamental para demonstrar que a evidência não foi comprometida (Oliveira, 2021).

O direito de punir, predito de forma genérica como ação exclusiva do Estado, torna-se factual quando é realizada uma infração, deliberada como crime na Lei Penal, originando uma pretensão punitiva, mediada pelo Ministério Público e conduzida em oposição ao infrator, que reagirá exercitando sua defesa (Fernandes, 2016).

Para responsabilizar um indivíduo a um determinado crime no direito processual penal é necessário a comprovação dos fatos ocorridos, assim como a verificação dos vestígios encontrados após a prática do mesmo (Medeiros, 2021). De acordo com a Lei nº 3.689 de 03 de outubro de 1941, Art. 158-A § 3º: “Vestígio é todo objeto ou material bruto, visível ou latente, constatado ou recolhido, que se relaciona à infração penal”.

Com o avanço tecnológico e as mudanças envolvendo o manejo de crimes, observa-se a necessidade de adaptação e mudança dentro do processo penal. Nesse sentido, os dados digitais vão de encontro a uma dessas mudanças. Estes por sua vez passam a ser também uma fonte probatória de determinados crimes (Das Almas, 2021).

A escolha deste tema justifica-se pela grande quantidade de notícias diárias de pessoas que sofrem com crimes virtuais, tornando-se uma realidade cotidiana, onde buscar por proteção legal é de extrema importância. Para além disso, justifica-se também pela necessidade de encontrar mecanismos de proteção para a custódia da prova digital.

Diante do exposto faz-se os seguintes questionamentos: Como garantir a inviolabilidade da prova digital para sua admissão no processo penal?

Diante disso, o objetivo geral deste estudo foi analisar o emprego da cadeia de custódia da prova digital e sua licitude, como meio de verificar quais os mecanismos utilizados para garantir a confiabilidade das provas digitais no processo penal.

Já os objetivos específicos foram compreendidos por: identificar quais as leis e normas que garantem a aplicabilidade da cadeia de custódia da prova digital; descrever quais os meios para a admissão da prova digital no processo penal; verificar qual a relevância e o peso da prova digital no esclarecimento de crimes; avaliar a importância da prova digital nos crimes da contemporaneidade.

Com o propósito de estudar os meios e licitudes da prova digital para sua admissão no processo penal e de adquirir uma resposta para os objetivos apresentados nesse artigo, foi realizada uma análise de produções através da pesquisa bibliográfica via internet através de artigos, periódicos e editoriais encontrados nas bases de dados SCIELO, Portal de Periódicos CAPES e Google Acadêmico, buscando compreender o que é dito pelos autores a respeito do tema abordado.

A pesquisa bibliográfica é uma busca nas bases de dados e na literatura fundamentada em proposições fundamentais que gerem o estudo científico. Geralmente, utiliza-se da internet para a realização de pesquisas em bases de dados com credibilidade científica, para que sejam obtidas produções bibliográficas que auxiliem no estudo e na elaboração de novas produções (Pizzani, 2012).

Além disso, também foi realizada uma pesquisa documental, abordagem de pesquisa que envolve a análise de documentos como fonte principal de dados.

Ao longo do trabalho, os tópicos de discussão compreendem a relação da evolução da tecnologia com a cadeia de custódia, onde evolução da tecnologia impacta diretamente a cadeia de custódia, exigindo adaptações constantes para garantir a integridade, autenticidade e admissibilidade das evidências, especialmente no contexto das provas digitais. A Lei 13.964/2019 que se refere ao Pacote Anticrime, visando aprimorar o combate à corrupção, ao crime organizado e aos crimes violentos e ABNT NBR ISO/IEC 27037:2013, norma técnica brasileira que aborda diretrizes para identificação, aquisição e preservação de evidências digitais em investigações forenses. E por último, o tratamento das evidências digitais, parte fundamental da investigação de crimes virtuais e os tipos de crimes

virtuais que envolvem atividades criminosas que são cometidas por meio de computadores e redes digitais.

1. EVOLUÇÃO TECNOLÓGICA E CADEIA DE CUSTÓDIA

Os incessantes progressos da tecnologia da informação acoplados à precisão de automatização insituicional, ocasionaram em uma nova demanda tecnológica, a utilização de documentos digitais. A adesão dessa maneira de registrar alastrou-se e acabou por ultrapassar as fronteiras do espaço de trabalho e já faz parte da rotina da sociedade (Dos Santos; Flores, 2020).

Com a revolução técnico-científica, diversos aspectos sociais também se modificaram. Frente a isso, o aumento da dependência de pessoas e empresas na utilização de sistemas e equipamentos pode ser notada, principalmente na última década. Não obstante dessa realidade, os crimes também obtiveram novos métodos para sua ocorrência, sendo nomeados os crimes nesse ambiente de crimes virtuais ou digitais. Corroborando com esse pensamento, segundo Lopes (2016, p.01):

> Desde a criação do computador e sua atribuição para facilitar os trabalhos humanos, é possível perceber sua grande evolução, bem como a velocidade em que são criadas novas soluções e equipamentos. Da mesma forma em que a tecnologia avança, os crimes que até então só eram praticados no mundo real agora começaram a ganhar outra forma, a forma virtual. Assim é possível afirmar que a necessidade de profissionais especialistas na área de investigação digital é mais do que imprescindível.

Para a comprovação desses crimes, existem alguns meios e critérios a serem seguidos, dentre eles pode-se citar a cadeia de custódia da prova digital, que é um conjunto de processos constituídos pela Lei 13.964/2019 do Código Penal. A prática desses procedimentos já é algo antigo nas Ciências Forenses, onde as evidências coletadas são manuseadas de maneira cautelosa e registradas na cadeia de custódia.

De acordo com Oliveira (2021) “independente da área de atuação, todas as amostras são recebidas como evidências, analisadas e o seu resultado é apresentado na forma de laudo, objetivando dissertar um parecer sobre a evidência examinada”.

Além disso, segundo Pastore e Da Fonseca (2022, p.99):

> A Cadeia de Custódia é considerada um conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte.

Ou seja, a aplicação da cadeia de custódia leva a redução de possíveis erros jurídicos, os quais podem acarretar condenações errôneas ou não condenações. Caso haja razões para uma quebra dessa cadeia de custódia, a confiabilidade dessa evidência comprometerá o processo de investigação criminal (Das Almas, 2021).

> O impasse inicia-se com popularização da internet, cumulada com a falta de conscientização da importância da prevenção, com a adoção de medidas de segurança, que podem refletir outra fragilidade da internet tornando a identificação do criminoso limitada. Por último, o Brasil detém de leis que buscam a proteção das pessoas físicas ou jurídicas que são vítimas de crimes cibernéticos, interessando o legislador na reivindicação dos direitos dos cidadãos, contudo seu alcance não e prosperado tratando-se de um crime transnacional de informática, por outro lado, a busca continua na eficácia da aplicação da ciência criminal no entendimento dos crimes cibernéticos, que para isso, caso seja regulamentar a responsabilidade do proprietário do equipamento emissor das informações, sendo que na impossibilidade de localizar o criminoso que utilizou o dispositivo informático para a execução do crime, responsabilizar-se-ia o proprietário da máquina (Oliveira, 2021, p. 13).

Dessa maneira, para o levantamento e análise dessas evidências com o objetivo de fins jurídicos, é necessário o trabalho de um profissional capacitado, sendo indicado um perito ou analista forense. Esses profissionais são escassos no ambiente de trabalho, mesmo com a grande demanda existente no mercado. Além disso, a computação forense é pouco explorada, dificultando consideravelmente essa área (Lopes, 2016).

Para a preparação de um exemplar de cadeia de custódia da prova digital, é necessário se atentar a algumas particularidades, como as evidências e os locais onde estão armazenadas essas evidências. Isso devido à volatilidade e complexidade dessa evidência, onde a mesma pode ser perdida ou modificada. Por isso a necessidade da cadeia de custódia da prova digital, contribuindo para que se identifique todas as etapas que essa evidência passou (Oliveira, 2021).

2. LEI 13.964/2019 E ABNT NBR ISO/IEC 27037:2013

Com o intuito de inserir na legislação algo que corroborasse com a importância de tal meio para o processo penal, foi promulgada a Lei n.º 13.964/2019, onde se fala sobre a cadeia de custódia e as etapas necessárias para a preservação da integridade da prova. No entanto, essa promulgação não menciona em momento algum sobre as provas imateriais, como no caso a cadeia de custódia referente as provas digitais. Além disso, o legislador relata que não caberia menção a isso, uma vez que os elementos eletrônicos estão em constante avanço tecnológico (Das Almas, 2021; Pastore; Da Fonseca, 2022).

A Lei 13.964/2019, conhecida como Lei Anticrime, constituiu uma pequena mudança na legislação penal) brasileira. Em seu texto a lei fala sobre a necessidade de seguir determinado protocolo com relação a cadeia de custódia, devendo ser seguida tanto por peritos criminais quanto pelos médicos legistas dos casos e processos. O capítulo II da referida lei em seu Art. 158-A, diz que:

> § 1º O início da cadeia de custódia dá-se com a preservação do local de crime ou com procedimentos policiais ou periciais nos quais seja detectada a existência de vestígio.
> § 2º O agente público que reconhecer um elemento como de potencial interesse para a produção da prova pericial fica responsável por sua preservação.
> § 3º Vestígio é todo objeto ou material bruto, visível ou latente, constatado ou recolhido, que se relaciona à infração penal.

No mesmo capítulo, em seu Art. 158-B, temos as seguintes etapas para o rastreamento do vestígio:

> I - reconhecimento: ato de distinguir um elemento como de potencial interesse para a produção da prova pericial; II - isolamento: ato de evitar que se altere o estado das coisas, devendo isolar e preservar o ambiente imediato, mediato e relacionado aos vestígios e local de crime; III - fixação: descrição detalhada do vestígio conforme se encontra no local de crime ou no corpo de delito, e a sua posição na área de exames, podendo ser ilustrada por fotografias, filmagens ou croqui, sendo indispensável a sua descrição no laudo pericial produzido pelo perito responsável pelo atendimento; IV - coleta: ato de recolher o vestígio que será submetido à análise pericial, respeitando suas características e natureza; V - acondicionamento: procedimento por meio do qual cada vestígio coletado é embalado de forma individualizada, de acordo com suas características físicas, químicas e biológicas, para posterior análise, com anotação da data, hora e nome de quem realizou a coleta e o acondicionamento; VI - transporte: ato de transferir o vestígio de um local para o outro, utilizando as condições adequadas (embalagens, veículos, temperatura, entre outras), de modo a garantir a manutenção de suas características originais, bem como o controle de sua posse; VII - recebimento: ato formal de transferência da posse do vestígio, que deve ser documentado com, no mínimo, informações

> referentes ao número de procedimento e unidade de polícia judiciária relacionada, local de origem, nome de quem transportou o vestígio, código de rastreamento, natureza do exame, tipo do vestígio, protocolo, assinatura e identificação de quem o recebeu; VIII - processamento: exame pericial em si, manipulação do vestígio de acordo com a metodologia adequada às suas características biológicas, físicas e químicas, a fim de se obter o resultado desejado, que deverá ser formalizado em laudo produzido por perito; IX - armazenamento: procedimento referente à guarda, em condições adequadas, do material a ser processado, guardado para realização de contra perícia, descartado ou transportado, com vinculação ao número do laudo correspondente; X - descarte: procedimento referente à liberação do vestígio, respeitando a legislação vigente e, quando pertinente, mediante autorização judicial.

Nesse sentido, todos os vestígios coletados durante o processo devem ser fielmente tratados como previsto na lei. Diante disso, para sanar esse abismo pode-se usar como base outros meios/protocolos redigidos pela Norma ABNT NBR ISO/IEC 27037:2013. Essa norma tem como objetivo a padronização no tratamento de evidências digitais, visando preservar a integridade da mesma. Oliveira (2021, p.1) fala ainda que essa norma: “contribuirá para obter sua admissibilidade, força probatória e relevância em processos judiciais ou disciplinares”.

Essa evidência digital é caracterizada ou produzida por diferentes meios podendo ser eles dispositivos digitais, equipamentos periféricos, celulares, computadores, banco de dados, entre diversos outros. Como esse tipo de material é qualificado como algo volátil e frágil a proposta de normas para seu manuseio é necessária, garantindo assim sua confiabilidade e autenticidade. Portanto, para fornecer credibilidade a todo o processo de investigação, a metodologia utilizada para obtenção dos resultados é primordial, tanto no que diz respeito ao tratamento da evidência, quanto aos profissionais que iram executar tais atividades (Oliveira, 2021).

É importante ressaltar que, mesmo não sendo prevista na legislação essa norma está de acordo com as leis vigentes e regulamentos internacionais. Sendo assim, é recomendado que a mesma não passe por cima de nenhuma jurisdição, mas sirva de apoio para prática de especialistas que atuam nesse tipo de investigação ou área (Oliveira, 2021).

3. TRATAMENTO DAS EVIDÊNCIAS DIGITAIS E TIPOS DE CRIMES VIRTUAIS

O Direito Processual Penal em um Estado Democrático de Direito, tem por desígnio, sempre de acordo com a Constituição Federal, adequar-se à intenção punitiva nascida com a execução do crime, concepção obsoleta e que minimiza a relevância da conduta adjetiva, mas, especialmente, tal qual o Direito Processual Penal, servir de ferramenta para assegurar direitos (Lobo, 2019).

O responsável pela ação penal é, verdadeiramente, o Ministério Público, porém, o juiz pode colaborar com o Ministério Público, atuando na busca e compilação de provas e decretando as medidas preventivas (Mendes, 2008).

> Com a difusão da internet, surgiram criminosos altamente especializados na linguagem informática, dando origem a uma variedade de termos para se referir às infrações penais realizadas por meio de dispositivos conectados à rede mundial de computadores. Essas terminologias abrangem cibercrimes, crimes cibernéticos, crimes informáticos, crimes na internet, crimes virtuais, crimes digitais, entre outros. Todos são sinônimos de ações criminosas que envolvem o uso de computadores e redes de computadores, incluindo ataques de negação de serviço (DDoS), fraudes bancárias e espionagem cibernética. No entanto, vale ressaltar que nem todas as ações ilegais realizadas na internet são consideradas cibercrimes. Este é um termo amplo que engloba não só atividades criminosas em rede, mas também comportamentos ilegais como cyberbullying, difamação e assédio online (DAS ALMAS, 2021, p.8).

O exercício desse controle da sociedade realizado pelo Estado também tem uma limitação, que é constituído pela reverência aos direitos humanos, que precisam ser considerados, em qualquer estudo que se realize do direito material e processual penal. Na Constituição Federal têm princípios que limitam o emprego do Direito Penal, proibindo penas de morte e perpétuas, proibindo provas ilícitas, a criminalização da tortura, a invasão de domicílios e os princípios da dignidade da pessoa humana e da presunção da inocência (Valle, 2009).

Salienta-se que o processo penal necessita demasiadamente da memória humana para a reconstituição dos fatos, visto que o crime já aconteceu, já está no passado, e só existe na memória. Além do mais, há casos onde a história da vítima ou da testemunha é a única prova através do reconhecimento de pessoas. Entretanro, é importante que não se esqueça os riscos que cercam esses casos, visto que, a mente humana está sujeita a distorcer alguns fatos sendo influenciada internamente e externamente (Badaró, 2015).

Normalmente, o reconhecimento de pessoas é utilizado na intenção de realizar a identificação e confirmação do autor do delito. Porém, ele é utilizado também para identificar a vítima ou a testemunha para certificar que, de fato, aquele indivíduo presenciou o delito (Rangel, 2015).

Diante do grande desafio que se tem ao trabalhar com as evidências digitais, são necessárias algumas precauções ao lidar com o manuseio, tratamento, armazenamento e análise desse material. Silva (2017, apud Pinheiro, 2009, p.174) afirma que: “Apesar do alto nível de precisão da computação forense, há uma fragilidade: a coleta das evidências. Coletar de forma errônea pode tornar ilícita ou invalida determinada prova”.

Frente a isso, para que esse material digital, seja buscado/investigado num sistema eletrônico é preciso que aconteça uma varredura minuciosa, uma vez que estes dados podem estar na forma de arquivos danificados ou mesmo deletados (Silva, 2017).

De acordo com Das Almas (2021, p.2):

> Destaca-se ainda que, diante da escassez de instrução dos responsáveis pela coleta de tal espécie probatória, os riscos referentes a interferências que acarretem a contaminação do material ou – em determinados casos – a coleta indevida de dados que não apresentam relação com a investigação em si, são excessivamente superiores, gerando a possibilidade do cometimento de erros jurídicos.

Para que a prova digital seja aceita, ela deve cumprir algumas normas específicas (gerais e técnicas) relacionada ao seu tipo, tratamento e sobre sua cadeia de custódia. Uma dessas normas diz respeito a norma técnica da ABNT ISO IEC 27037:2013, onde em resumo são propostos os seguintes procedimentos para a cadeia de custódia das evidências digitais:

> I- a devida identificação dos dispositivos de armazenamento de mídia digital e aqueles que podem conter evidência digital relevante;
> II- a coleta da evidência digital, que será removida da localização original em que ocupa e será remetida a um ambiente controlado;
> III- a aquisição, consistente na produção de cópia da evidência digital e documentação dos métodos utilizados;
> IV- a preservação da evidência, consistente na proteção desta contra possíveis adulterações. (ABNT, 2013).

As etapas da investigação forense para as evidências digitais são classificadas em seis momentos, sendo elas a aquisição (coleta), preservação,

extração, recuperação, análise e apresentação. Durante a coleta dos dados o profissional capacitado para o serviço sempre trabalhará com a cópia do material, isso por que caso esse arquivo seja corrompido, o original estará intacto. Ainda nesse momento, para que esse material seja preservado de maneira integral é requerida sua cadeia de custódia (Silva, 2017; Lopes, 2016).

Após isso, é realizado o exame dos dados colhidos na primeira fase com o intuito de localizar, filtrar e extrair as informações que auxiliem no processo em andamento. Na etapa seguinte esses dados ou informações são analisadas de maneira minuciosa para responder as perguntas do inquérito. Por fim, se tem a apresentação dos resultados encontrados por meio de um relatório. Nesse sentido, de acordo com Silva (2017, p.6):

> Para garantir estes princípios os peritos precisam documentar todas as suas ações, determinar e aplicar um método para estabelecer a precisão e confiabilidade das evidências digitais; e reconhecer que o ato de preservação da prova digital potencial não pode ocorrer sempre de maneira não-invasiva.

Com relação ao seu tratamento, as evidências digitais devem seguir algumas condições, entre eles pode-se citar: auditabilidade, repetibilidade, reprodutibilidade e justificabilidade. O primeiro diz respeito ao procedimento ou técnica utilizada e se a mesma foi adequada para o caso, já o segundo garante que se tenha os mesmos resultados por meio da reprodução da mesma técnica feita anteriormente. O terceiro, é caracterizado pela produção de mesmos resultados quando utilizado diferentes instrumentos ou condições. Por fim, o quarto tem o intuito de justificar os meios utilizados para o tratamento da evidência digital (Lopes, 2016).

> As três condições previstas na NBR ISO/IEC 27037:2013, são: Relevância: demostrar que o material adquirido é relevante para a investigação. Confiabilidade: os processos utilizados na manipulação de evidências digitais em potencial devem ser auditáveis e repetíveis. Suficiência: material suficiente deve ser recolhido (Silva, 2017, p.6).

As provas digitais são caracterizadas e inseridas no processo penal como provas científicas imateriais, onde para ocorrer a troca de informações e de dados tem-se a utilização dos meios eletrônicos (Das Almas, 2021).

Para a produção da prova digital deve-se estabelecer maior cautela, uma vez que, suas características são completamente diferentes das provas materiais, tendo maior fragilidade e vulnerabilidade. Por conta disso, essas provas se tornam mais fáceis e passíveis de contaminação, falsificação e/ou destruição (Badaró, 2021).

Nesse processo de obtenção de provas, reverbera o questionamento sobre os procedimentos realizados perante a cadeia de custódia das mesmas, buscando a veracidade do material probatório. Nesse sentido, é através do protocolo meticuloso de manuseio desse material que proporciona a defesa e/ou acusação desse indivíduo ao crime averiguado (Sobrinha, 2021).

Assim, ao analisar a inserção cada vez maior da tecnologia no campo investigativo do direito, percebe-se a necessidade da criação de procedimentos específicos pertinentes ao registro e manuseio desses elementos, garantindo sua legalidade, preservação e licitude como parte dos vestígios no processo penal. Além disso, salienta-se que na contemporaneidade não pode existir diferenciação na validação de provas imateriais e materiais, inexistindo explicação para que a cadeia de custódia abranja apenas elementos materiais (Machado, 2022).

Ou seja, a cadeia de custódia da prova digital se faz cada vez mais necessária para fazer parte do processo e comprovar as informações relacionadas. Além de fazer com que o material obtido seja verídico e confiável, ela também possibilita questionar o mesmo quando não manuseado de maneira correta e irrefutável (Badaró, 2021; Machado, 2022).

Primeiramente, é importante que seja entendido que existe uma diferença entre hackers e crackers. O hacker é aquele que detém conhecimento e prática avançados na área da computação e da internet. Porém, ele usa esse conhecimento para favorecer a justiça e combater os criminosos virtuais. Em contrapartida, os crackers são os criminosos que praticam atos ilícitos no ambiente virtual (Viana; Machado, 2013).

O processo é o fundamento em que se propaga a consolidação da tutela jurisdicional. Considerando o direito penal como última razão, o processo penal ganha aspectos de interface que tem a capacidade de apresentar a confirmação jurídica para aperfeiçoamento da criação e materialidade de um crime, de forma que concretizem os direitos básicos garantidos na constituição a cada sujeito (Silva, 2017).

> Focalizando-se a Internet, há dois pontos de vista a considerar: crimes ou ações que merecem incriminação praticados por meio da internet e crimes ou ações que merecem incriminação praticados contra a Internet, enquanto bem jurídico autônomo. Quanto ao primeiro, cabe observar que os tipos penais, no que concerne à sua estrutura, podem ser crimes de resultado de conduta livre, crimes de resultado de conduta vinculada, crimes de mera conduta ou formais (sem querer discutir se existe distinção entre estes) e crimes de conduta com fim específico, sem prejuízo da inclusão eventual de elementos normativos. Nos crimes de resultado de conduta livre, à lei importa apenas o evento modificador da natureza, com, por exemplo, o homicídio. O crime, no caso, é provocador o resultado morte, qualquer que tenha sido o meio ou a ação que o causou (Greco Filho, 2000, p. 95).

Associando com esse propósito, o processo penal que deriva no início do pagamento da tutela jurisdicional apropriada traz, como decorrência social, o recuo do desassossego à ordem pública ocasionado pela prática delitiva (Silva, 2017).

Os crimes virtuais são práticas ilícitas executadas por meios tecnológicos, como computador e celular com internet. Estes podem ser classificados de acordo com a sua forma de cometimento. Entre os principais estão: crimes de pornografia infantil, discriminação, crimes contra a honra, estelionato, fraudes bancárias e pirataria (Assunção, 2021).

Leonardi (2012) e Soares (2012) dissertam que os crimes digitais são caracterizados como acessos não autorizados a sistemas tecnológicos que acabam por destruir, modificar, infringir direitos autorais, incitar o ódio, praticar a intolerância religiosa, divulgar pornografia infantil, usar dos dados do proprietário do equipamento digital para fazer ameaças, dentre outros.

Assunção (2021, p.8), resume as características de alguns desses crimes como:

> A pornografia infantil caracteriza-se pelo ato de fotografar ou publicar cenas de sexo explícito que contenham crianças ou adolescentes, nos moldes do art. 241 do ECA. Injúria, difamação e calúnia são considerados crimes contra a honra e estão regulamentados nos artigos 138, 139 e 140 do Código Penal. No ambiente da internet, os crimes de calúnia e difamação, consideradas ofensas à honra objetiva, são caracterizados caso a ofensa seja enviada para grande público e não somente para a vítima, já se tratando de injúria, considerada ofensa à honra subjetiva, a ofensa é direcionada para a própria vítima. Tratando-se do crime de estelionato no ambiente da internet, o sujeito ativo mantém a vítima em erro, sob a finalidade de obter vantagem ilícita para si próprio. Também se considera crime cibernético exaltar ou elogiar criminoso ou ato criminoso de maneira pública, caracterizando crime de apologia de crime ou de criminoso. Outro exemplo, consiste no oferecimento, utilizando a internet, de consumo a

> substância entorpecente, ou que sujeite a pessoa a depender-se fisicamente ou psicologicamente, caracterizando tráfico de drogas.

Exemplo disso, foi o caso ocorrido com a atriz Carolina Dieckmann em 2012, onde criminosos virtuais tentaram extorquir a quantia de R$ 10 mil reais dela sob a ameaça de divulgarem suas fotos íntimas que a atriz guardava em seu e-mail e que eles tiveram acesso. Como a atriz não cedeu as ameaças e não pagou o valor, suas fotos foram divulgadas e o crime foi configurado como interceptação de e-mail e extorsão (Franck; Ferreira, 2023).

Diante disso, foi criada a Lei nº 12.735/12, mais conhecida como Lei Carolina Dieckmann:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

A Lei Carolina Dieckmann foi fundamental para o despertar das autoridades e da sociedade para a preocupação com crimes ocorridos na internet. Porém, ainda há muito o que se discutir e a se colocar em prática, pois, o ataque cibernético, além de causar constrangimento e dor de cabeça, pode gerar problemas mais graves como ansiedade e depressão o que pode fazer com a vítima pense até em mesmo em suicídio (Brigida, 2017).

Nesse sentido, para se fazer valer a lei contra esses tipos de crimes, é necessária uma evidência digital do ocorrido. A partir daí todo o processo de coleta e análise desses dados vai de encontro ao tema do presente trabalho.

O impasse enfrentado tanto no Brasil como em outros países, é descobrir de que maneira os crimes virtuais podem ser combatidos e como conseguir trazer segurança aos usuários que armazenam arquivos pessoais e sigilosos em seus dispositivos eletrônicos, que ultrapassa as fronteiras espaciais e permite que o crime seja cometido virtualmente, dificultando a prisão dos criminosos (Oliveira, 2021).

> Um dos fatores que impossibilitam esse combate é que a internet permite o anonimato, o que dificulta a identificação do autor, haja vista a possibilidade de manipulação desses dados, outro sim, são os flagrantes que também é quase impossível de ser acontecido, pois, muitas das vezes, o resultado crime vem muito depois do início de alguma execução, pois a vítima muito

> das vezes só reconhece o prejuízo após um grande lapso temporal, não imediatamente à sua execução (Assunção, 2021, p. 12).

Por meio dos recursos tecnológicos a aquisição de provas é cada vez mais utilizada nos ambientes, isso porque, a cada postagem, tem um caso que pode ser utilizado no processo penal, entretanto, os progressos que são localizados nos crimes virtuais, quase não são encontrados no mundo cibernético, pois existem obstáculos em diversas camadas do direito (Badaró, 2021).

> Diante da evolução tecnológica existe uma predisposição social em reconhecer bens jurídicos informáticos e, dentre os que mais se sobressaem, temos o sigilo e a segurança de dados e informações eletrônicas. Para a autora, é tal juízo de reprovação (violação a dados e a informações privadas) que move o Direito Penal. De fato, tal juízo de reprovação existia, mas foi preciso que uma pessoa pública, atriz popular, fosse vítima de um suposto crime informático para que o legislativo finalizasse uma discussão de mais de 10 (dez) anos no Congresso Nacional, com a aprovação da Lei n. 12.737/2012, sancionada em 30 de novembro do mesmo ano (Machado, 2022, p.6).

Existem diversos projetos de lei tramitando no Congresso Nacional que tem por objetivo caracterizar como crime esse tipo de comportamento ilícito com a utilização da tecnologia e dispositivos eletrônicos. Consequentemente, esse modelo de projeto de lei não só descreve o processo penal, como, direciona outros dispositivos já inclusos no instrutivo penal instituídos pelo Código Penal, assim como observa as normas da Convenção Internacional de Budapeste, criada em 2004, que discute a respeito dos crimes virtuais (Sobrinha, 2021).

> Sob esse panorama, o compromisso do Brasil com a Convenção de Budapeste no combate ao cibercrime, introduz a cooperação indispensável para a perseguição e punição efetiva desses delitos, além das fronteiras nacionais, incentivando a cooperação jurídica internacional. Tal adesão representa um marco importante para a promoção da democracia e a proteção dos direitos humanos, considerando a carência de uma legislação moderna e específica para combater os cibercrimes no Brasil (Silva, 2017, p. 18).

É necessário que sejam estabelecidas novas orientações voltadas para a proteção de dados, principalmente quando esses dados são pessoais, sigilosos e/ou com sensíveis. Por mais que existam esforços para garantir a segurança virtual do indivíduo, ainda há fragilidades no que concerne ao ambiente jurídico. Diante disso,

ressalta-se que tem uma carência de legislação exclusiva sobre determinados assuntos voltados aos crimes cibernéticos, como a escassez de uma alimentação exclusiva de registro das denúncias e o despreparo de particularidades na esfera estadual (Medeiros, 2021).

Nesse panorama, se confirma uma divergência entre a legislação e a população, resultado da rapidez com que as mudanças na tecnologia acontecem. A celeridade com que as informações são transitadas, atrelada ao anonimato concedido por esses mecanismos, torna a legalidade ainda mais incitadora. Dessa forma, a legislação brasileira tem se deparado com empecilhos para acompanhar o desenvolvimento dos crimes cibernéticos, expondo brechas que podem ser ocupadas em espaços como segurança de dados, vigilância e cooperação internacional (Dos Santos; Flores, 2020).

CONSIDERAÇÕES FINAIS

Perante a pesquisa bibliográfica que foi realizada nesse estudo e os resultados que foram alcançados, percebeu-se que todo conteúdo de dados e informações que são armazenados em dispositivos tecnológicos são sigilosos, pois culminam em incumbências dos princípios da intimidade e da vida privada.

Diante da leitura dos estudos, percebeu-se que os dados e informações armazenados em dispositivos digitais foram protegidos pelo Código Penal, que decretou como crime a invasão à privacidade individual, tanto de pessoa física, quanto de pessoa jurídica.

Destaca-se que, mais do que aperfeiçoar e especializar, é preciso investir em equipamentos para comporem as Delegacias de Polícias e Núcleos de Criminalísticas para que seja possível atender as demasiadas demandas de crimes digitais.

Portanto, torna-se necessário que sejam realizadas trocas de saberes nas Faculdades de Direito, bem como, nos locais de trabalho, juntamente com a população, para que todos conheçam e tomem conhecimento a respeito do tema.

Diante do exposto, notou-se que as vítimas de crimes virtuais passam por muito sofrimento, desrespeito, crueldade e covardia quando a sua intimidade é invadida por crackers e exposta para a sociedade sem pudor e sem escrúpulos.

Pode-se perceber que a luta para assegurar proteção aos crimes cibernéticos é árdua e demorada, pois, mesmo que já existam Leis que regem para proteger a sociedade contra criminosos virtuais, ainda assim, é falha e demorada. Entretanto, graças a criação da Lei Carolina Dieckmann, hoje as vítimas têm mais força e coragem de denunciar os criminosos, e a Polícia Judiciária tem meios para punir.

Algumas hipóteses observadas e levantadas no decorrer da pesquisa e escrita do presente trabalho, foram: a rápida evolução da tecnologia que impacta a coleta, preservação e admissão de provas digitais no processo penal; os desafios associados à autenticidade e integridade das provas digitais e como a correta preservação e documentação da cadeia de custódia é crucial para garantir a admissibilidade de evidências digitais no tribunal.

Conclui-se, então, que o desenvolvimento da internet resultou em um avanço simultâneo no número de crimes por meio dessa rede mundial de computadores ou cometidos por meio de outra tecnologia computacional. Dessa forma, novas tecnologias também foram e devem continuar a ser pesquisadas para automatizar a procura e a persecução penal de criminosos na internet, além de uma melhoria nas ferramentas atualmente disponíveis para agências de forças de lei, o que pode ser obtido com uma integração de pesquisas.

Por fim, é importante que os governos, as universidades e as indústrias entendam as mudanças no modus operandi dessas atividades criminais, trabalhando continuamente em conjunto para desenvolver novas tecnologias e soluções de investigação, que melhorarão a performance da tecnologia disponível para encontrar materiais íntimos de uma maneira forense e com um correto estabelecimento da cadeia de custódia.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSUNÇÃO, Ayume da Silva. A tipicidade dos crimes cibernéticos no direito penal brasileiro: Um estudo sobre o impacto da Lei nº 12.737/2012 e a (des) construção de uma dogmática penal dos crimes cibernéticos. 2021. 16f. Trabalho de conclusão de curso (Bacharel em Direito). Centro Universitário Faculdade Guanambi. Bahia, 2021

BADARÓ, Gustavo. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. **Boletim IBCCRIM**, v.29, n. 343, p.1-7, 2021.

BADARÓ, Gustavo Henrique. Processo Penal. 3. ed. São Paulo: **Revista dos Tribunais**, 2015.

BRIGIDA, Ingrid Sassen Paz Santa. Aspectos processuais penais dos crimes digitais: meios de produção de prova e a Teoria da Cadeia de Custódia. **Trabalho de Conclusão de Curso (Bacharelado em Direito)-Faculdade Nacional de Direito, Universidade Federal do Rio de Janeiro, Rio de Janeiro**, 2017.

DAS ALMAS, Amanda Costa. A aplicabilidade da cadeia de custódia em dados digitais utilizados como prova no processo penal brasileiro. **Boletim IBCCRIM**, v.30, n. 343, p.1-30, 2021.

DOS SANTOS, Henrique Machado; FLORES, Daniel. Cadeia de custódia digital arquivística. **LexCult: revista eletrônica de direito e humanidades**, v. 4, n. 2, p. 108-139, 2020.

FRANCK, Kewry Mariobo; FERREIRA, Romario Vitorino. Instruções preventivas contra crimes cybernéticos e orientações da perícia forense computacional. **NATIVA-Revista de Ciências, Tecnologia e Inovação**, v. 4, n. 1, p. 116-132, 2023.

GRECO, Vicente Filho. Algumas observações sobre o direito penal e a internet. **Boletim IBCCRIM**, v. 8, p. 3, 2000.

LEONARDI, Marcel. **Tutela e Privacidade na Internet**. São Paulo: Saraiva, 2012.

LOBO, Jorge. Hermenêutica, interpretação e aplicação do Direito. **Revista do Ministério Público do Estado do Rio de Janeiro**, nº 72, abr./jun. 2019.

LOPES, petter Anderson. FORENSE DIGITAL – COMPUTAÇÃO FORENSE. PERÍCIA FORENSE COMPUTACIONAL. 2016.

MACHADO, Fernando Alves. **A cadeia de custódia e a prova penal digital.** 2022. 85f. Trabalho de conclusão de curso (Bacharel em Direito). Universidade Pederal do Pampa. Rio Grande do Sul, 2022.

MARIANO, Ari Melo; ROCHA, Maíra Santos. Revisão da literatura: apresentação de uma abordagem integradora. In: **AEDEM International Conference**. p. 427-442, 2017.

MEDEIROS, Fernando Henrique Canedo de. **A cadeia de custódia à luz do pacote anticrime como forma de resguardar a prova pericial no processo penal.** 2021. 36f. Trabalho de conclusão de curso (Bacharel em Direito). Faculdade Evangélica de Goianésia. Goianésia, 2021.

MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional, 2º ed., São Paulo: Saraiva, 2008, p. 149.

OLIVEIRA, Vinícius Machado de. A Cadeia de Custódia em Provas Digitais. 2021.

PASTORE, Alexandro Mariano; DA FONSECA, Manoel Augusto Cardoso. Cadeia de Custódia de Provas Digitais nos Processos do Direito Administrativo Sancionador

com a adoção da tecnologia Blockchain. **Cadernos Técnicos da CGU**, v. 3, n. 1, p.97-109, 2022.

PIZZANI, L. et al. **A arte da pesquisa bibliográfica na busca do conhecimento.** Revista Digital de Biblioteconomia e Ciência da Informação, v. 10, n. 2, Campinas– São Paulo, 2012.

RANGEL, Paulo. Direito Processual Penal. 23ª ed. São Paulo: **Atlas**, 2015.

SANTOS, Adriano José Sousa; BORGES, André Felipe Miranda; RODRIGUES, Gustavo Luís Mendes Tupinambá. A cadeia de custódia na coleta da prova digital de acordo com a lei 13.964/2019, dos seus artigos 158-a ao 158-f. **RECIMA21-Revista Científica Multidisciplinar-ISSN 2675-6218**, v. 2, n. 8, p. e28612-e28612, 2021.

SILVA, Tamara Bruna Ferreira da. Perícia digital: estratégias para analisar e manter evidências íntegras em forense computacional. **Gestão da segurança da Informação-Unisul Virtual**, v.1, n.1, p.1-15, 2017.

SILVA, Marco Antonio Marques. Processo penal e Estado Democrático de Direito. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Processo Penal. Marco Antonio Marques da Silva (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017.

SOARES, Murilo Cesar. **Os Direitos Na Esfera Pública Mediática: a Imprensa como instrumento da Cidadania**. São Paulo: Cultura Acadêmica, 2012.

SOBRINHA, Maria Quaranta de lobão. **Cadeia de custódia das provas digitais: a perícia técnica como instrumento das garantias**. 2021.71f. Trabalho de conclusão de curso (Bacharel em Direito). Universidade Federal de Sergipe. Sergipe, 2021.

VALLE, Dirceu Augusto da Câmara et al. **Prisão e liberdade no processo penal militar**. 160 p. 2009. ~

VIANA, Tulio; MACHADO, Felipe. **Crimes informáticos**. Belo Horizonte: Fórum, 2013.

VIEIRA, Antonio. A cadeia de custódia da prova no processo penal: algumas notas sobre as alterações promovidas pela Lei 13.964/2019 (Pacote Anti Crime). **Boletim bimestral Trincheira Democrática do Instituto Baiano de Direito Processual Penal**, v. 3, n. 7, p.27-32, 2020.