JNT-FACIT BUSINESS AND TECHNOLOGY JOURNAL ISSN: 2526-4281-QUALIS B1
ANO 2023 – MÊS DE AGOSTO - FLUXO CONTÍNUO - Ed. 44. Vol. 01. Págs. 178-194

CAPES

CNPq
Conselho Nacional de Desenvolvimento Científico e Tecnológico

Facit.TO
FACULDADE DE CIÊNCIAS DO TOCANTINS

CRIMES CIBERNÉTICOS: DESAFIOS DA INVESTIGAÇÃO E PRESERVAÇÃO DAS PROVAS

CYBER CRIMES: CHALLENGES OF INVESTIGATION AND PRESERVATION OF EVIDENCE

Elison de Araújo FREITAS
Faculdade de Ciências do Tocantins (FACIT)
E-mail: adv.elison.freitas@faculdadefacit.edu.br
ORCID https://orcid.org/0009-0006-863-1451

Pedro Henrique Aguiar SILVA
Faculdade de Ciências do Tocantins (FACIT)
E-mail: adv.pedro.silva@faculdadefacit.edu.br
ORCID https://orcid.org/0009-0007-4606-1297

Márcio Cabral de SOUZA
Faculdade de Ciências do Tocantins (FACIT)
E-mail: Marcio.souza@faculdadefacit.edu.br
ORCID https://orcid.org/0009-0009-7058-704

RESUMO

O presente artigo trata do cenário de dificuldades enfrentadas pela força de investigação no recolhimento e preservação de evidências digitais como meios de prova substanciais ao processo de decisão e elucidação dos fatos ocorridos em espaços virtuais como único caminho a comprovação, ou não, de crimes cibernéticos. Para isso foi explorada a definição de crime cibernéticos considerando como marco de análise as características inerentes do tipo como a volatilidade de informações e dados que sejam suficientes ao rastreio e conexão do sujeito ativo com o ato contra o sujeito passivo, abordando a dinâmica destes sujeitos no interim das peculiaridades cibernéticos. Seguidamente são elucidadas as normas referentes a obtenção de provas, meios de prova e requisitos e limitações aos quais estão submetidos os instrumentos de investigação, considerando também a atipicidade do meio virtual e, por fim, o estudo avança a abordagem do conceito de evidências digitais, sua importância e a dificuldade de sua obtenção devido a lacunas legais e a dualidade de facilitação versus entraves gerados pelo Marco Civil da Internet na obtenção e preservação de evidências digitais. O método de pesquisa aplicado foi o bibliográfico qualitativo totalmente fundamentado

no estudo de doutrina clássica somada a produção acadêmica mais recente em relação ao tema central de obtenção e preservação de provas na investigação do crime cibernético.

Palavras-Chave: Cibercrimes. Provas. Evidências digitais.

ABSTRACT

This article deals with the scenario of difficulties faced by the research force in the collection and preservation of digital evidence as substantial evidence for the decision-making process and elucidation of the facts that occurred in virtual spaces as the only way to prove, or not, cyber crimes. For this, the definition of cyber crime was explored, considering as a framework for analysis the inherent characteristics of the type, such as the volatility of information and data that are sufficient for tracking and connecting the active subject with the act against the passive subject, addressing the dynamics of these subjects in the interim of cybernetic peculiarities. Next, the norms referring to obtaining evidence, means of proof and requirements and limitations to which the research instruments are subject are elucidated, also considering the atypicality of the virtual environment and, finally, the study advances the approach to the concept of digital evidence, its importance and the difficulty of obtaining it due to legal loopholes and the duality of facilitation versus barriers generated by the Civil Rights Framework for the Internet in obtaining and preserving digital evidence. The research method applied was the qualitative bibliographic fully based on the study of classical doctrine added to the most recent academic production in relation to the central theme of obtaining and preserving evidence in the investigation of cybercrime.

Keywords: Cybercrimes. Evidences. Digital evidence.

INTRODUÇÃO

É inegável a magnitude que os avanços da tecnologia alcançaram, desde seu surgimento até os dias atuais a rede conhecida como internet gerou diversas mudanças para a vida da sociedade global como um todo, em diversos aspectos é fácil apontar a inerente necessidade que hoje existe em relação a habitar espaços virtuais, seja em

virtude de trabalho, seja como lazer, seja para questões financeiras e afins a presença das tecnologias de comunicação atreladas a internet é parte fundamental aos processos sociais.

A normalização do convívio virtual gerou certo conforto inesperado, diversos sujeitos rapidamente perceberam que era possível explorar tal ambiente como anônimos, esse elemento somado a ausência de legislação voltada ao local fez com que uma onda de crimes fosse instaurada. Tais crimes são comumente chamados de cibercrimes, se fundamentam principalmente nas dificuldades que a força investigativa enfrenta para recolher provas que sejam suficientes para instauração do processo penal.

O ponto chave do presente artigo é compreender as compatibilidades, e incompatibilidades, entre o conceito de prova tradicional e o recolhimento de evidências nos meios virtuais, atravessando desde a conceituação do crime cibernético, a compreensão dos sujeitos, ativo e passivo, e suas posições, principalmente abordando as formas pelas quais o sujeito ativo consegue evitar conexão com o ato.

Passado esse ponto o estudo avança a abordagem dos meios de prova, seu conceito tradicional e aplicabilidade aos casos práticos, considerando-a como elemento base a solução de conflitos, no tocante ao objeto enquanto influenciador do processo de decisão, responsabilização e fixação de pena.

Enfim o estudo elenca as dificuldades enfrentadas nos parâmetros dos ambientes virtuais com base no recolhimento e manutenção de evidencias, a localização real em contrapartida dos programas criados para dissimular os dados de rastreio, levando em conta os métodos de investigação cibernética após o Marco Civil da internet, com foco especifico a identificação e a manutenção de evidencias virtual como provas únicas deste tipo criminal.

CONCEITUANDO CRIMES CIBERNÉTICOS

Para se chegar ao conceito do que se entende sobre crimes cibernéticos, foi necessário definir seus termos de acordo com a normatividade, enquadrando na teoria do conceito analítico finalista do crime, como sendo condutas típicas, antijurídicas e culpáveis, aos quais são praticadas com a utilização dos sistemas de informática, sendo

a motivação por diferentes questões, sejam políticas, fins econômicos ou satisfação pessoal (SCHMIDT, 2014).

Conforme a Convenção sobre Cibercrimes em 2001, em Budapeste, informa algumas definições sobre esse tema, trazendo o conceito de sistema informativo, *modo operandi* do sujeito ativo, em seu art. 1º, alínea a, como "qualquer dispositivo isolado ou um grupo de dispositivos relacionados e interligados, me que um ou mais de entre eles, desenvolve, em execução de um programa, o tratamento automatizado dos dados" (CONVENÇÃO SOBRE CIBERCRIME, 2001, p. 3).

Ainda, no mesmo documento, na alínea b, sobre a terminologia de dados informativos, definindo como:

> […] qualquer representação de fatos, de informações ou de conceitos sob uma forma susceptível de processamento num sistema de computadores, incluindo um programa, apto a fazer um sistema informativo executar uma função (CONVENÇÃO SOBRE CIBERCRIME, 2001, p. 3)

Já na definição de cibercrime, a convenção (2001), traz o conceito como atos praticados contra a confidencialidade, integridade e disponibilidades de sistemas informativos, de redes e dados, assim como a utilização por meio de fraudes desses sistemas, redes e dados.

Mesmo com essas premissas, há outros conceitos que devem ser estudados, já que há um entendimento próprio por cada autor.

Fabrizio Rosa (2002) trabalha com o conceito de crime cibernético como sendo:

> A conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; 2. O „Crime de Informática" é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. Assim, o „Crime de Informática" pressupõe does elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrá-los; 4. A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5. Nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento

> automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc. (ROSA, 2002, p. 53)

Ainda, a autora Patricia Peck Pinheiro conceitua os crimes virtuais em duas modalidades, a depender da proteção do bem jurídico tutelado. Na primeira, pode-se utilizar o exemplo do crime de interceptação de dados, no qual o Bem jurídico são os dados, requerendo a proteção da transmissão, coibindo o uso dessas informações para fins culposos (PINHEIRO, 2007), esses são conhecidos como crime cibernético próprio.

Já na segunda modalidade, se chama crime cibernético impróprio, nessa questão, o agente ativo usa a internet como o *modo operandi* para praticar outras finalidades, com violações de bens jurídicos comuns, como por exemplo, fraude, estelionato, crimes contra a dignidade sexual, entre outros (PINHEIRO, 2007).

Para Barreto e Silva, os autores conceituam a ideia de crime cibernético como um aquele que envolve o uso de tecnologias, seja computador, internet ou caixas eletrônicos, usando tal instrumento como um crime meio, para outro fim, ou seja, a forma que é praticada se torna inovadora (2016, p. 36).

Após entender sobre a terminologia dos crimes cibernéticos, é necessário enquadrar as características do sujeito ativo. Na pesquisa feita por Glenny (2008), o agente é em sua maioria composto por homens, com pouca habilidade de comunicação, ou seja, não possui um ciclo social abrangente, tendo aprendido a prática do craking na faixa etária entre os 13 aos 15 anos de idade, ou seja, por volta da adolescência, onde o individuo tende a encontrar desafios sociais, sem ter consolidado ainda seus valores morais, no qual o mundo virtual passa a ser seu quarto de interação, sem que precise interagir diretamente com outras pessoas.

Entretanto, em uma investigação policial, esse estereótipo não deve ser focado como estudo justamente por causa do acesso as informações para todos, desta forma, qualquer pessoa pode ser um criminoso cibernético (BARRETO; SILVA, 2016, p. 43).

A própria rede de internet é uma ferramenta onde há técnicas de aprendizagem para pratica de crimes, de qualquer natureza, principalmente quando há zonas como a

deep web em que não se há rastro quanto aos dados reais dos usuários devido o anonimato.

No ambiente virtual, deve separar dois tipos de pessoas, a primeira, conhecida como hackers, possuem um conhecimento abrangente sobre informática e segurança de redes, utilizando a proteção e defesa dos menos favorecidos. Esses são conhecidos como White hats (chapéus brancos), já os crackers, esses utilizam seus conhecimentos para praticar crimes delituosos, também chamados como Black hats, ou chapéus pretos (BARRETO; SILVA, 2016, p. 44).

No Brasil, a atuação dos criminosos cibernéticos é intensamente desenvolvida, pois na internet há a possibilidade do indivíduo localizar todos os tipos de serviços, como por exemplo, a criptografia para hospedagem, programação, virais no facebook, dentre outros (ASSOLINI, 2016 *apud* BARRETO; SILVA, 2016, p. 43).

Para Paesani (2010), o perfil dos criminosos desse tipo penal apresenta o sentimento de autoconfiança, assim como o sentimento de anonimato e impunidade, ainda mais porque a interação com a vítima acontece indiretamente, em locais distantes um do outro, sem um contato direto com a mesma.

Em um estudo feito por um especialista italiano da Polícia do Estado (STRANO), o mesmo afirma o seguinte:

> Essa nova modalidade de criminosos informáticos é composta por sujeitos não violentos e solitários, que cometem crimes que não cometeriam fora do espaço cibernético. Isso inclui o perfil das pessoas mais variadas. Para essas pessoas, a tela do computador funciona como escudo de proteção que se projeta no mecanismo do pensamento; ou seja, a falta de percepção da ilegalidade do comportamento, dos riscos assumidos e do dano causado à vítima (PAESANI, 2010, s/p, on line).

Em virtude disso, devido ao acesso facilitador da rede de comunicações em uma escala global, justamente com esses sentimentos de autoconfiança e o anonimato presente para os usuários, as informações e dados compartilhados são falsos, se tornando difícil de colher provas para suficiência de autoria e comprovação da materialidade do delito.

No ordenamento jurídico brasileiro, para que o indivíduo seja punida, a conduta do mesmo deve ser típica, antijurídica e culpável. Além disso, é necessário que tenham provas suficientes para incriminar o agente. Caso haja dificuldade na investigação

policial, não haverá vestígios e coleta de dados para o andamento do processo, em virtude do princípio do contraditório, da ampla defesa e do in dúbio para o réu.

A localização do sujeito ativo é crucial para a investigação, justamente porque o crime é consumado em uma rede de internet, onde a vítima e o agente estão distantes, sem contato direto. O anonimato interfere na identificação dos responsáveis, consequentemente, não há comprovação de autoria e materialidade (AMARAL, 2022).

MEIOS DE PROVA APLICÁVEIS AO PROCESSO PENA

As provas são elementos importantíssimos desde as civilizações mais antigas, visto que com o passar dos anos, o homem se adaptou a viver em uma sociedade regida por leis penais, ou seja, em que o direito penal vem a promover uma sociedade mais organizada, ao qual defende a coletividade.

A prova é o meio utilizado durante a persecução penal, para o reconhecimento da verdade e persuasão do juiz. Visto que, a procura pela verdade real e evidente acolhimento dos fatos criminosos e sua autoria. A prova se torna um elemento indispensável, pois pode ser usada de forma direta e indireta para mostrar o que está sendo alegado no decorrer do processo.

Sendo um meio importante no decorrer do processo penal, as provas são baseadas por princípios norteadores, que disciplinam seu uso. Sendo eles: princípio da autorresponsabilidade das partes; princípio da liberdade de provas; princípios da imediação e prova ilícita por derivação.

Os meios de provas existentes estão de forma não taxativa no Código de processo penal, que traz e seu Título VII, dos artigos 155 a 250, os meios de provas utilizados. Todavia, a doutrina visa organizar os tipos de provas existentes de acordo com cada classificação.

Em relação as provas em espécie, elas são encontradas no Código de processo penal, sendo elas: a perícia (arts. 158 a 184 do CPP), que se trata de um documento elaborado por peritos, como resultado do que se foi periciado, tendo a finalidade de registrar informações singulares sobre a matéria de fato, ao ponto de que o juiz possa se utilizar dela como prova técnica; interrogatório (arts. 185 a 196 do CPP), é ato que visa tanto a autodefesa do acusado, como também é um meio de prova, já que ele está inserido no CPP.

Sendo assim, pode ser produzido a qualquer tempo, ao ponto de ser permitida a renovação do ato a todo o tempo da persecução penal, desde que seja de ofício pelo juiz ou a pedido das partes; confissão (arts. 197 a 200 do CPP), é o ato pelo qual o acuso no processo penal, reconhece em juízo os fatos que a ele foram atribuídos, ou seja, como ``a expressão designativa da aceitação, pelo autor da prática criminosa, da realidade da imputação que lhe é feita´´ (Mirabete); declaração do ofendido (art. 202 do CPP), é um dos meios de prova, pelo qual o juiz ouvira a oitiva do ofendido, pois através dele é viável o fornecimento de informações em relação ao fato criminoso; testemunhas (arts. 202 a 225 do CPP), são as pessoas que estão estranhas a relação jurídica, tendo como prova, a narração dos fatos que tenham presenciado na hora da prática do delito; reconhecimento de pessoas e coisas (arts. 226 a 228 do CPP), é o meio de prova, pelo qual uma pessoa irá reconhecer outra ou afirma a veracidade de uma coisa.

A acareação (arts. 229 e 230 do CPP) é um ato processual que está em conflito, logo são colocadas frente a frente as pessoas que fizeram declarações sobre um mesmo fato, porém os atos contados estão divergindo entre si; documentos (arts. 231 a 238 do CPP), é o meio de prova que é constituído especialmente para servir como prova dos atos que estão sendo ali julgados ou investigados; indícios (art. 239 do CPP), é a todo ato que pode ser conhecido ou provado, e que se chega a conclusão da existência de outro fato, sendo assim, toda prova indiciaria tem o mesmo valor que qualquer outra.

Uma vez que, é através das provas diretas ou indiretas que se busca provar a verdade real. O que difere os meios de provas de um crime físico, para os meios de provas em relação aos cibercrimes, devido as diversas facilidades de atuação dos criminosos cibernéticos, seja pela falta de estrutura estatal ou pelo ciberespaço ser um local que facilita a eliminação das provas.

Sendo de grande importância o reconhecimento do autor do crime, nasce a necessidade de traçar o perfil dos criminosos cibernéticos, que veem a ser denominados de hacker. E determinada importância de reconhecer o autor que praticou o delito, e dada pela doutrina jurídica clássica, sob a ótica de que para existir uma sanção penal, é indispensável que não se tenha dúvidas sobre quem praticou o crime e sua autoria, não podendo assim, a lei chegar a uma pessoa abstrata, que no caso em foco, seria o virtual.

Como já relatado acima, prova é a busca pela verdade real, e nos crimes físicos já é bastante difícil a produção de provas, e em se tratado do cibercrime as dificuldades são bem maiores, visto que, as infrações cometidas no ciberespaço raramente deixam rastros, fazendo assim com que, o seu autor fique encoberto no anonimato.

Devido as provas ilícitas seguirem os mesmos passos das demais, elas deveram ser desmembradas do processo, porque violam o art. 5, LVI da CF/88, em razão de que para se iniciar uma investigação criminal na rede é necessário a prévia autorização judicial. Uma vez que, os cibercrimes são instáveis e fáceis de serem apagados ou alterados, além de poderem ser cometidos de qualquer lugar do mundo.

Em função dessa facilidade de alteração de provas sobre os cibercrimes, é de bom tom que ao iniciar as investigações seja delimitada a ferramenta que foi utilizada para o cometimento do delito. Podendo os cibercrimes, serem cometidos através de correios eletrônicos, e-mails, websites, programas maliciosos (vírus), programas de transferência de informações, redes sociais, sites de comércio eletrônico (e-commerce), devido a essa variedade de ferramentas, é necessário ter em foco qual foi a utilizada no cibercrime, já que as técnicas para investigação são diferentes.

Logo, em virtude da facilidade das provas serem adulteradas e apagadas, uma das opções para manter essas provas são a solicitação de preservação de registro de provedor de conexão ou solicitação de preservação de registro de aplicação de internet. Dessa forma, um dos meios de provas que podem ser utilizados para a confirmação dos crimes virtuais, são a certidão do escrivão de polícia e a ata notarial, onde a primeira é regida pelo CPC em seu arts. 439 a 441.

Em seu art. 439, do CPC dispõe sobre "a utilização de documentos eletrônicos no processo convencional dependerá de sua conversão a forma impressa e da verificação de sua autenticidade, na forma da lei". Enquanto isso, a ata notarial vem com a finalidade de determinar a existência de um fato que é relevante para o judiciário. Segundo Didier, Braga e Oliveira (2015, p. 214):

> Por se tratar de documento público, a ata notarial faz prova não só da sua formação, mas também dos fatos que o tabelião declarar que ocorreram em sua presença (art. 405, CPC). Quando utilizada em juízo, no entanto, é preciso ter em mente que se trata, normalmente, de meio de prova produzido unilateralmente.

Contudo, mesmo que os meios de provas para a confirmação dos crimes virtuais, seja de difícil produção, nos dias atuais já existem delegacias especializadas em crimes cibernéticos, não é à toa que se vem surgindo novas legislações para amparar as vítimas de determinados crimes, e uma dessas legislações pertinentes e a Lei Carolina Dieckamnn de nº 12.723/2012, ao que é uma alteração no Código Penal Brasileiro, que acrescenta os arts. 154-A e 154-B, e ainda altera os artigos 266 e 298 do mesmo código.

Ao final, é nítido que a internet vem crescendo de forma assustadora nas últimas décadas e determinado crescimento não ficou apenas aliado aos computadores, mas as novas tecnologias que não parem de ser lançadas, como os smartfones e tablets, logo, a possibilidade de crimes virtuais acontecerem vem se ampliando e tomando proporção maiores, o que dificulta ainda mais a obtenção de provas concretas, para a confirmação dos crimes cometidos no âmbito cibernético.

DESAFIO DA REUNIÃO DE PROVAS APLICÁVEIS AO PROCESSO PENAL

Conseguir provas frente a crimes cibernéticos realmente se mostrou um desafio maior do que a produção legislativa conseguia acompanhar, de fato, sendo considerada a última década sozinha os avanços legais foram impulsionados pelas situações delituosas. É necessário entender a base elementar da prova virtual, que é a evidência digital.

De acordo com o Manual de Investigação Cibernética, lançado após a publicação do Marco Civil da internet, evidência digital é o elemento crucial da investigação tal qual sua correlata evidência física em locais de crime, contudo é muito mais inconstante e anônima, inicialmente, facilmente modificada, escondida, redirecionada ou mesmo eliminada (BARRETO; BRASIL, 2016, p. 51).

Pequenos instrumentos do software dos dispositivos utilizados quando alterados podem gerar grandes complicações, o Manual exemplifica arquivos temporários, horários e datas como exemplo de evidências digitais, vestígios que comprovem os fatos.

Preservar dados como esses é um dos maiores desafios enfrentados pela investigação judiciária e a devida persecução penal, então como igualar o procedimento natural de vítima busca a delegacia para denúncia, são recolhidas evidências e com indícios suficientes aberto o processo, levantadas provas sólidas para

o esclarecimento dos fatos e enfim influenciar a decisão, se no começo da jornada já existe o impedimento das evidências simplesmente não existirem.

Isso faz com que se retorne a raiz do conceito dos meios de prova enquanto instrumentos adequados a dar a convicção da veracidade ou não de um fato (GRECO, 2010, p. 188). É Denilson Feitoza (2010) que afirma que não devem existir limitações para os meios de prova, melhor expressando, para a obtenção de provas de acordo com os já previstos no Código de Processo Penal e legislações específicas, ou não, sendo a lógica aplicada muito clara, a única limitação real é o respeito ao texto constitucional e as leis.

O próprio Código de Processo Penal não determinou um rol taxativo para a obtenção dos meios de prova presentes nos artigos 158 e seguintes, isso podendo ser identificado no mesmo código no art. 155, parágrafo único, que determina uma limitação em relação às restrições à avaliação do estado físico-psicológico das pessoas, ou seja, o exame de corpo e delito (FERREIRA, 2020, p. 17).

Quais seriam as limitações à obtenção de meios de prova digitais, e caso não baste essa pergunta pode ser possível avançar e dizer quais seriam os problemas em utilizar os meios disponíveis que sejam coerentes à realidade do combate aos crimes cibernéticos.

Diante das peculiaridades do ambiente é inegável que as medidas para recolher evidências serão extensivas (DOMINGOS, 2017), e por saber que cada mínimo elemento pode ser uma evidência virtual é que devem ser levados em conta não apenas dispositivos físicos, mas também mecanismos como o *cloudcomputing* que é o armazenamento de dados diversos no sistema de nuvem, ou seja, os arquivos guardados não estão atrelados a uma única maquina, ficam reservados em espaço da rede e podem ser acessados e compartilhados a distância por meio de quase todo tipo de dispositivos (LOPES, 2017, p. 20).

Assim se chega a um ponto chave, o que é a evidência digital em si e o que ainda é apenas o arquivo de dados, no caso do primeiro os dados já estão separados e protegidos para que não sofram alterações, já são tidos como comprovação, enquanto o segundo são dados sendo mantidos e protegidos mais que ainda estão sendo recolhidos, ou mesmo produzidos (BARRETO; BRASIL, 2016, p. 51).

Considerando o armazenamento em nuvem como método de armazenagem de dados sem atrelamento a um único dispositivo faz com que para a obtenção de provas não baste meramente recolher dispositivos onde tenham sido identificados a abertura de dados conectados a investigação, equipamentos podem ser furtados o que tornaria confuso suspeitar do dono original do dispositivo, sendo este o único com dados registrados na máquina.

Exemplificando a situação vem o caso emblemático de 2012 em que o radialista e humorista Rodrigo Vieira, o Mução, famoso nas rádios do norte e nordeste foi preso no estado de Pernambuco sob a acusação de pedofilia por meio da Operação Dirtynet movida pela Polícia Federal, contudo a prisão havia sido feita apenas com base na conexão da propriedade dos dispositivos com o humorista, na realidade o real autor dos crimes que chegou a confessar fora seu irmão que tinha completo acesso a computadores, tablets e afins que pertenciam ao radialista (CORREIO DO ESTADO, TERRA, 2012).

A situação fora completamente baseada no rastreio de IP que conectou a propriedade dos objetos ao humorista e radialista, considerando o tipo penal em questão é compreensível à urgência da investigação, mas pelas mesmas razões deve ser visto que as evidências não seriam suficientes para que houvesse indícios de veracidade dos fatos, como apontado pelo Manual de Investigação Cibernética é preciso avaliar mesmo os menores elementos como evidências virtuais.

Nesse momento é devido avançar para a preocupação quanto à preservação da evidência enquanto fundamento ao processo, tratando da realidade volátil dos dados online não se deve negar que o usuário que verdadeiramente realiza o delito através do uso do espaço virtual pode, com muita facilidade, mascarar sua identidade ou mesmo redirecionar a culpabilidade fazendo com que seja de difícil ou até impossível a individualização de autoria e materialidade delitiva (BARRETO; BRASIL, 2016, p. 52).

A reunião de evidências digitais, e sua preservação nesta condição, é um procedimento muito mais trabalhoso do que aquele requerido aos crimes físicos principalmente pela característica de volatilidade do meio virtual, não basta que a investigação encontre um dispositivo pelo qual tenha sido compartilhado o conteúdo delitivo, ou que obtenha o rastreio dos dispositivos utilizados quando se tratar de

arquivos de dados em nuvens, é necessário que faça a conexão entre agente e instrumentos utilizados, configurando as evidências por completo.

O passo a passo a ser seguido deve ser feito para que a credibilidade, a autenticidade, a integridade e a originalidade das informações preservadas sejam a própria reprodução dos dados originais, identificando a pegada digital que o real agente deixe como vestígio.

No entanto, como dito anteriormente obter as evidências digitais não é tarefa fácil, garantir sua preservação menos ainda, diferentemente de evidências e vestígios físicos as digitais são facilmente manipuladas, extintas, modificadas no tempo que normalmente a investigação física levaria para alcançar provas, somado a isso está o fato de que durante muito tempo a balança entre crimes cibernéticos e legislação especifica ao tema esteve muito desequilibrada, com grandes lacunas em relação a procedimentos, garantias e deveres da investigação virtual.

É com essa motivação que o Marco Civil adentrou a legislação brasileira, sob a lei 12.965 de 2014, todavia não ter sido um texto voltado à investigação de cibercrimes ainda sim gerou grandes impactos no tema, inclusive estabelecendo prazos, requisitos e limitações aos procedimentos da investigação cibernética (BARROSO, 2019, p. 40).

As opiniões são muito controversas em relação à forma como o Marco Civil afetou a tratativa com o meio virtual, se por um lado ocasionou certas dificuldades de acesso aos dados cadastrais e aos registros de acesso (GONÇALVES DA SILVA, 2022, p. 29), por outro lado capacitou o requerimento cautelar que objetiva a preservação dos registros de conexão, acessos e aplicações de internet (BARRETO; BRASIL, 2016, p.52).

A questão é justamente sobre a rapidez na qual é possível ter acesso a certas informações e urgentemente preserva-las a título de evidência digital, e nesse interim o art. 10, §1º do Marco Civil determina que provedores tem o dever obrigatório de fornecer os registro de acesso que permitam a identificação do usuário, mas somente com apresentação de ordem judicial, enquanto que de acordo com o Decreto regulamentar do Marco Civil nº 8.771 de 2016 os dados cadastrais, quais sejam a qualificação pessoal e profissional, não atentam contra o direito a privacidade ou ao sigilo de comunicação (GONÇALVES DA SILVA, 2022, pp. 29-30-31).

O enfrentamento é claro, a investigação fica sujeita a um nível de urgência e celeridade absurdo devendo impreterivelmente recolher informações que sejam

evidencias digitais de autoria e materialidade, preserva-las como tal e ainda dentro dos prazos legais devem reunir mais outras evidências que confirmem a identificação do sujeito, porém submete-se a obtenção de ordem judicial para cada registro de acesso ou conexão, fazendo com que todo o procedimento siga aos tropeços.

Cabe apenas à autoridade responsável enfrentar a burocracia para com urgência requisitar a preservação daqueles dados enquanto evidências digitais para delimitar o perfil de atuação do agente investigado, e só assim sustentar provas solidas a tomada de decisão. Mesmo com os entraves gerados pelo Marco Civil da Internet é por essa mesma norma que foram conquistados a medida cautelar e a urgência nos procedimentos para que sejam preservadas as evidências digitais.

Contudo os procedimentos de preservação de evidências digitais ainda estão truncados e a falta de observação destas gera as situações como o exemplo dado em virtude do elemento anônimo do meio virtual. Se for através de evidências digitais com base em dados cadastrais e acessos de registro e conexão, a acessibilidade aos mesmos no intuito de obtenção de prova deve passar por uma reestruturação, afinal o proposito da evidência digital é muito claro e sua ausência é extremamente perigosa. Dessa forma é possível ver que a evolução legislativa está cada vez mais próxima, mas ainda assim tem um longo caminho a percorrer na tratativa da obtenção de provas e dos meios de prova.

CONSIDERAÇÕES FINAIS

Neste artigo, buscou-se compreender sobre a dificuldade durante as investigações policiais com relação as provas produzidas nos crimes cibernéticos onde o anonimato predomina no perfil dos usuários, sem que deixe rastros no cometimento dos seus crimes, ao ponto de sairem impune em virtude dessa dificuldade.

Primeiramente, foi trazido o conceito de crimes cibernéticos, citados por diferentes autores da área, como um fato típico, antijuridico e culpável, onde a internet é o meio instrumental que o sujeito ativo utiliza para cometer os atos delituosos. Ainda, para entender sobre o crime cibernético, é necessário compreender sobre o perfil do criminoso, onde sua autoconfiança se predomina justamente pelo anonimato, podendo ser qualquer pessoa capaz, com acesso as informações e dados.

Após, com esse pontapé, tem-se a questão das provas utilizadas para buscar a identificação dos usuários, sejam provas dentro do processo penal, como provas do cibercrimes. Essa comunicação auxilia na coleta de dados a fim de reconhecer o sujeito ativo que atua dentro da rede de comunicações.

Em seguida, é trabalhada a questão da dificuldade de obtenção de provas nos meios virtuais, considerando os entraves legais aos meios de provas naturais deste tipo penal, que são as evidencias digitais. Em virtude da volatilidade do ambiente virtual fundamentada na facilidade de alteração ou meio, exclusão de dados de informações somado a questão da possibilidade de ser anonimo, o cenário acaba sendo mais prejudicado pela burocracia judiciária e pelos bloqueios das lacunas legais, fazendo com que o atual enfrentamento contra crimes cibernéticos seja muito mais dificultoso em relação ao recolhimento e preservação das evidencias digitais, que são os únicos meios de provas úteis a investigação cibernética.

Por fim, os meios tradicionais de obtenção de provas, quando aplicados sem a atenção das evidências digitais, facilmente podem ser a ruina da investigação cibernética quando ignoram as evidências digitais, causando erroneamente a junção de autoria e materialidade em um sujeito ou sujeitos que apenas sejam proprietários de dispositivos que tenham sidos utilizados para perpretar o ato criminoso ou mascarar outros dispositivos utilizados na criminalidade como o exemplo trabalhado.

REFERÊNCIAS

ALENCAR, Mariana. **Crimes Cibernéticos e Meios de Prova.** Jusbrasil, 2016. Disponível em: https://mariiialencar.jusbrasil.com.br/artigos/643636447/crimes-ciberneticos-e-meios-de-prova#:~:text=O%20cybercrime%20pode%20ocorrer%20com,as%20t%C3%A9cnicas%20para%20investiga%2Dlo. Acessado em: 08 de janeiro de 2023.

AMARAL, Jean Carlos Rossafa. **Crimes cibernéticos e as dificuldades no processo de investigação para os crimes na internet**. Publicado em 24 de maio de 2022. Disponível em: https://conteudojuridico.com.br/consulta/artigo/58454/crimes-cibernticos-e-as-dificuldades-no-processo-de-investigao-para-os-crimes-na-internet#:~:text=E%20as%20maiores%20dificuldades%20encontradas,ausente%20a%20autoria%20e%20a. Acesso em: 14 de jan. 2023.

Convenção sobre Cibercrime. Budapeste. Publicado em 23 de junho de 2001. P. 14. Disponível em: https://rm.coe.int/16802fa428. Acesso em: 12 de jan. 2023

BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética a luz do Marco Civil da Internet**. Brasport Livros e Multimídia LTDA. Publicado em 2016;

BARROSO, Carolina Rodrigues de Carvalho. **Meios de investigação e produção de provas nos crimes cibernéticos.** Universidade Federal Fluminense, Niterói, 2019.

CORREIO DO ESTADO, Terra. **Humorista acusado de pedofilia é solto; irmão assume crimes.** Publicada em: 30 de junho de 2012. Disponível em: <https://correiodoestado.com.br/cidades/humorista-acusado-de-pedofilia-e-solto-irmao-assume-crimes/153398/> Acessado em: 14 de janeiro de 2023.

CORTEZ, André Vieira. **Produção de Provas nos Crimes Cibernéticos.** Âmbito Jurídico, 2021. Disponível em: <https://ambitojuridico.com.br/cadernos/direito-penal/producao-de-provas-nos-crimes-ciberneticos/> Acessado em: 08 de janeiro de 2023.

DOMINGOS, F T S. A obtenção de provas digitais na investigação dos delitos de violência e exploração sexual infantil online. In: Silva, ARI, editor. **Crimes Cibernéticos.** Porto Alegre: livraria do advogado; 2017. pp. 235-54.

DIAS, Daniel Lélis. **Os meios de prova no processo penal brasileiro e sua importância.** Jusbrasil, 2016. Disponível em: <https://danielhc.jusbrasil.com.br/artigos/219666930/os-meios-de-prova-no-processo-penal-brasileiro-e-sua-importancia> Acessado em: 08 de janeiro de 2023.

DIDIER JR, F; BRAGA, P, S; OLIVEIRA, R, A. **Curso de Direito Processual Civil:** Teoria da Prova, Direito Probatório, Ações Probatórias, Decisão, Precedente, Coisa Julgada e Antecipação dos Efeitos da Tutela. 10 ed. Salvador: Ed. Jvspodium, 2015.

FEITOZA, Denilson. **Direito processual penal: teoria, crítica e práxis**. Niterói: Impetus, 2008.

FERREIRA, Vívian Crystina Silva. **Análise da Infiltração Virtual de Agentes Policiais para a Repreensão de Crimes Contra a Dignidade Sexual.** 2020. Disponível em: http://dspace.unilavras.edu.br:8080/server/api/core/bitstreams/afcac446-9a88-44c0-afdb-f64b96700364/content. Acesso em: 09 de jan. 2023.

GRECO FILHO, Vicente. **Manual de Processo Penal.** Saraiva, São Paulo, 2010.

GLENNY, Misha. **McMáfia: o crime organizado sem fronteiras**.Porto: Civilizacao Editora, 2008.

LOPES, Marisa da Silva Prado. **Crimes sexuais contra a dignidade sexual, através do uso da internet:** uma revisão crítica à legislação. Marisa da Silva Lopes. Universidade do Estado do Rio de Janeiro, Rio de Janeiro 2017.

MIRABETE, Júlio Fabbrini. **Processo penal**. 8 ed. São Paulo: atlas, 1999.

ROSA, Fabrizio. **Crimes de Informática**. Campinas: Bookseller, 2002. P. 53.

SCHIMIDT, Guilherme. **Crimes Cibernéticos**. Jusbrasil, publicado em 2014. Disponível em: https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos. Acesso em: 13 de jan. 2023;

PAESANI, Liliana Minardi. O papel do direito contra o crime cibernético. In: **Âmbito Jurídico,** Rio Grande, XIII, n. 79, ago.2010. Disponivel em: <http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=7972>.Acesso em: 8 de jan. 2023;

SILVA, Dickson Carvalho Gonçalves da. **Crimes cibernéticos:** limites e desafios da investigação. 2022. Disponível: repositorio.undb.edu.br/bitstream/areas/834/) Acesso em: 27-ago-2023.