DESAFIOS JURÍDICOS EM CRIMES CIBERNÉTICOS: competência, autoria, materialidade e provas digitais

Ana Luisa da Silva Nunes[1]
Wesley Wadin Passos Ferreira de Souza[2]

RESUMO
Este artigo explora a criminalidade digital em alguns de seus aspectos mais instigantes. Após contextualizarmos o leitor com a expressão crimes cibernéticos e apresentarmos uma classificação de suas formas de revelação, abordamos as principais questões sobre a definição da competência jurisdicional para o seu processo e julgamento e, em seguida, nos dedicamos a introduzir alguns pontos sobre a prova de sua autoria e materialidade. No que diz respeito às provas, concluímos, por meio da pesquisa bibliográfica, ser fundamental observar todos os passos da cadeia de custódia, sendo exigível a autorização judicial para adoção de diversas medidas capazes de invadir a esfera da privacidade dos investigados.

PALAVRAS-CHAVE: Crimes cibernéticos. Competência. Autoria. Materialidade. Provas digitais.

ABSTRACT
This article explores digital crime in some of its most intriguing aspects. After contextualizing the reader with the expression cybercrimes and presenting a classification of their forms of disclosure, we address the main questions about the definition of jurisdictional competence for their process and judgment and, then, we dedicate ourselves to introducing some points about the proof of its authorship and materiality. With regard to evidence, we concluded, through bibliographical research, that it is essential to observe all steps of the chain of custody, and judicial authorization is required for the adoption of various measures capable of invading the sphere of privacy of those being investigated.

KEYWORDS: Cyber crimes. Competence. Authorship. Materiality. Digital evidence.

SUMÁRIO

1 O DIREITO PENAL NA ERA DIGITAL. 2 MUDANÇA DE PARADIGMA ENTRE CRIMES MATERIAIS E CRIMES CIBERNÉTICOS NO DIREITO PENAL. 2.1 UMA ANÁLISE DA CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS. **3 COMPETÊNCIA PARA O PROCESSO E JULGAMENTO DOS CRIMES CIBERNÉTICOS. 4 AUTORIA E MATERIALIDADE NOS CRIMES CIBERNÉTICOS. 5**

[1] Graduanda em Direito pela Faculdade de Direito do Vale do Rio Doce (Fadivale). Estagiária na 2ª Vara Criminal da Comarca de Governador Valadares (MG).
[2] Doutor em Ciências da Comunicação pela Unisinos (RS). Mestre em Direito e Instituições Políticas pela FUMEC-BH. Graduado em Ciências Militares com ênfase em Segurança Pública no Curso de Formação de Oficiais - Polícia Militar do Estado de Minas Gerais. Graduado em Direito pela Faculdade de Direito Milton Campos. Atualmente é professor de Direito Processual Penal e Direito Constitucional na Fadivale. Magistrado Federal - Tribunal Regional Federal da Primeira Região desde 2003, tendo atuado como Promotor de Justiça em Minas Gerais entre 1998 e 2002 e como Oficial da PMMG entre 1994 e 1998. Áreas de pesquisa: Direito Processual Penal, Constitucional, Previdenciário e proteção ao consumidor, mudanças na visibilidade do Poder Judiciário na sociedade em midiatização e regulamentação do audiovisual brasileiro.

APONTAMENTOS GERAIS SOBRE O "*HASH*" COMO MEIO DE PROVA NOS CRIMES CIBERNÉTICOS. 6 CONCLUSÃO. REFERÊNCIAS.

1 O DIREITO PENAL NA ERA DIGITAL

A sociedade, ao longo dos anos, passou por vários processos de adaptação e se desenvolveu com base em necessidades únicas que serviram como fator determinante para se estabelecer a maior parte dos acontecimentos históricos.

Atualmente, a humanidade vive um novo momento, em que a cada instante, têm-se tópicos novos para se inteirar: a era digital. Dessa maneira, orientada por um novo meio de organização das informações que são transmitidas e alteradas a cada clique, as pessoas desenvolvem suas diversas maneiras de comunicação e interação social, apoiadas em recursos tecnológicos que permitem tais trocas sem a necessidade de estarem fisicamente presentes no mesmo local e, muitas vezes, de forma assíncrona.

Nesse sentido, Bioni (2019, p. 34) complementa:

> Essa nova forma de organização social foi sedimentada em razão da evolução tecnológica recente, que criou mecanismos capazes de processar e transmitir informações em uma quantidade e velocidade jamais imaginável. Os relacionamentos sociais foram energizados por um fluxo informacional que não encontra mais obstáculos físicos distanciais.

Neste contexto, destaca-se que a informação emergiu como um pilar fundamental na estruturação da sociedade contemporânea, oferecendo uma nova base de sustentação que impulsiona a conexão e o intercâmbio de narrativas e vivências. Esta transformação tem como objetivo primordial fortalecer os vínculos interpessoais, criando uma teia de relações mais estreitas e significativas entre os indivíduos.

No entanto, à medida que a tecnologia avança rapidamente, é notável que uma parcela significativa da população ainda não consegue acompanhar esse ritmo de maneira segura e informada. Esse descompasso torna esses indivíduos vulneráveis a uma imensidade de ameaças digitais, perpetradas por criminosos que exploram as lacunas na compreensão e na prática de segurança cibernética, para obterem maciços lucros ou objetivos socialmente reprováveis de forma muito insidiosa.

Pode-se dizer que a experiência mundial no período pandêmico da COVID-19 aprimorou o uso da internet e dos meios de comunicação no sentido de proporcionar melhor interatividade entre as pessoas, já que o momento não permitia contato físico. Nesse cenário, é inegável o impacto da tecnologia na sociedade durante tal momento. Dessa forma, a implantação acelerada de soluções tecnológicas trouxe inúmeros benefícios para todos os indivíduos, permitindo a continuidade de atividades e o acesso a serviços essenciais de forma remota.

No entanto, essa mesma expansão tecnológica também contribuiu para o surgimento de novas práticas ilícitas e possibilitou diferentes formas de execução de crimes já previstos no Código Penal.

Nesse contexto, o ciberespaço se tornou ambiente fértil para a prática de ilícitos, eis que através dele as noções de tempo e espaço são colocadas em xeque.

A emergência do ciberespaço torna útil esclarecer que estamos tratando de crimes ocorridos fora de um ambiente físico onde os fenômenos costumam aflorar. A ideia remete a um ambiente formado pela interconexão de sistemas de computadores e redes de comunicação, um espaço intangível, onde a informação é a principal moeda de troca e a comunicação é instantânea, permanente e global. As fronteiras físicas perdem relevância e as interações entre pessoas, máquinas e dispositivos se tornam cada vez mais comuns e intensas, desencadeando novas tensões da definição do tempo das coisas.

O termo ciberespaço foi cunhado pelo escritor William Gibson em seu livro "Neuromancer", publicado em 1984, e desde então tem sido amplamente usado para descrever a imersão humana no mundo digital. Nele, é possível encontrar uma infinidade de recursos, serviços e informações, acessíveis a partir de qualquer lugar do mundo, desde que se tenha conexão com a Internet.

Em outro momento já tivemos a oportunidade de abordar a definição trazida pela Unesco, mencionada por Kaminski:

> O ciberespaço é um novo ambiente humano e tecnológico de expressão, informação e transações econômicas. [...] Consiste em pessoas de todos os países, de todas as culturas e linguagens, de todas as idades e profissões fornecendo e requisitando informações; uma rede mundial de computadores interconectada pela infraestrutura de telecomunicações que permite à informação em trânsito ser processada e transmitida digitalmente (Kaminski 2002, p. 40 *apud* Souza 2023, p. 56).

No ciberespaço, as fronteiras entre palpável e o imaterial se misturam, criando novas formas de interação social, econômica e cultural. Redes sociais, comércio eletrônico, jogos online, serviços de streaming e muitas outras atividades são parte integrante desse universo digital em constante expansão. Desenvolve-se uma verdadeira cibercultura que põe em questão os limites dos diversos campos sociais, entre os quais o Direito, que assim como a Comunicação Social, busca controle de diversos aspectos da vida dos indivíduos e organizações.

Contudo, o ciberespaço também apresenta desafios e questões complexas relacionadas à segurança, privacidade, controle de dados e desigualdades de acesso, pressionando autoridades e usuários a clamar por proteção, especialmente em relação à privacidade, à intimidade, à honra objetiva e ao patrimônio. Não à toa, um dos temas que mais se debate atualmente é a necessidade de regulamentação da internet.

Em suma, o ciberespaço representa um novo paradigma de interação e comunicação, que se tornou fundamental em nosso cotidiano, sendo um espaço dinâmico, multifacetado e em constante evolução, que molda e é moldado pelas práticas e relações humanas na era da informação e da tecnologia.

2 MUDANÇA DE PARADIGMA ENTRE CRIMES MATERIAIS E CRIMES CIBERNÉTICOS NO DIREITO PENAL

Atrelado ao desenvolvimento acelerado da tecnologia em âmbito mundial, tem-se uma sociedade cada vez mais conectada e vulnerável frente às ações de criminosos que migraram suas práticas delitivas para o novo ambiente intangível, aperfeiçoando diversos delitos já existentes no Código Penal, sendo possível perceber que se abriu uma porta para a prática de crimes contra os usuários.

Essas ações ilícitas exercem um impacto direto e abrangente sobre a vida privada, financeira e coletiva das pessoas e o rol de crimes cibernéticos só está crescendo, como, estelionato, extorsão, roubo de dados bancários e informações pessoais, pornografia infantil, dentre outros.

Os crimes cibernéticos, de acordo com Cardoso (2023, p. 14), são a “conduta típica e ilícita praticada por meio de um computador, tablet, smartphone e uso da

internet, mesmo sem estar conectado a ela, ou seja, qualquer meio eletrônico que possa prejudicar terceiros".

As motivações predominantes por trás dos crimes cibernéticos no Brasil abrangem uma variedade de fatores, sendo os principais deles os ganhos financeiros ilícitos, a espionagem industrial, o hacktivismo e até mesmo a atuação de grupos criminosos organizados. Além disso, a facilidade de anonimato oferecida pelo ambiente online torna ainda mais desafiador o processo de identificação e responsabilização dos perpetradores dessa modalidade delitiva.

Após indicar o conceito de ciberespaço e de crimes cibernéticos é necessário diferenciá-los dos crimes que produzem efeitos no mundo físico, já que cada vez mais, têm passado a produzir resultados no mundo digital. Assim, Avelar (2019, p. 1, grifo nosso) apresenta inicialmente o conceito de crime material, formal e de mera conduta:

> **Crime material:** é aquele que prevê um resultado naturalístico como necessário para sua consumação. São exemplos o delito de aborto e o crime de dano. Há quem o chame de crime de resultado. **Crime formal:** é aquele que descreve um resultado naturalístico, cuja ocorrência é prescindível para a consumação do delito. Também denominado de delito de tipo incongruente. É o caso da extorsão mediante sequestro e o do descaminho. **Crime de mera conduta:** é aquele cujo resultado naturalístico não pode ocorrer, porque sequer há a sua descrição. Podemos tomar como exemplo o crime de ato obsceno, assim como o de violação de domicílio.

Ou seja, nos crimes materiais, a consumação está diretamente ligada ao resultado ou evento naturalístico exigido pelo tipo penal, ou seja, a uma mudança no mundo fenomênico. Nos crimes formais, a ação do agente consuma o delito independentemente da produção de efeitos no mundo exterior, embora ainda haja resultado ou evento jurídico.

Porém, conforme nos lembra Rossini (2004 *apud* Cardoso, 2023, p. 16) nos crimes cibernéticos a conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, omissiva e praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, de forma a ofender, direta ou indiretamente, a segurança informática, que tem por elementos a integralidade, a disponibilidade e a confidencialidade.

Os crimes cibernéticos constituem uma nova espécie de criminalidade que se coloca paralelamente aos delitos formais, materiais e de mera conduta. Na verdade,

eles podem se verificar de diversas maneiras a ponto de produzir ou não efeitos visíveis no mundo fenomênico ou apenas efeitos verificáveis no ciberespaço.

Assim, podemos afirmar que há delitos cibernéticos formais, materiais e de mera conduta. O que há de inovador no conceito é o fato de que os meios informáticos possibilitam a realização das condutas à distância, causando muito mais dificuldade na identificação dos infratores, do local do crime e do momento da realização dos atos executórios.

Convém mencionar que no ambiente digital os crimes ocorrem de forma remota, na maior parte dos casos, através de dispositivos eletrônicos e redes de computadores, explorando vulnerabilidades tecnológicas para acesso indevido a informações pessoais, financeiras ou corporativas. Eles podem envolver ataques cibernéticos, visando principalmente ganhos financeiros, espionagem industrial ou até mesmo causar danos a sistemas e infraestruturas essenciais.

Por outro lado, no mundo material, os crimes ocorrem em espaços físicos e geralmente envolvem violência física, roubo, agressão sexual, entre outros. Esses delitos impactam diretamente a integridade física e emocional das vítimas, além de trazerem consequências tangíveis no ambiente social, como medo e insegurança nas comunidades afetadas.

Embora os crimes cibernéticos não deixem marcas físicas visíveis, eles podem causar danos significativos em termos de perda de dados, violação de privacidade e prejuízos financeiros, evidenciando a complexidade e a necessidade de abordagens específicas para lidar com os desafios apresentados por ambos os cenários.

2.1 UMA ANÁLISE DA CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS

A classificação dos crimes cibernéticos é um tema de extrema relevância no contexto atual, em que a tecnologia desempenha um papel central em praticamente todas as esferas da vida humana. Estabelecer uma estrutura classificatória para esses delitos é fundamental para compreender a complexidade e a diversidade das atividades criminosas perpetradas no ambiente digital.

A categorização dos crimes cibernéticos pode ser feita de diversas maneiras, levando em consideração aspectos como os métodos utilizados pelos criminosos, os

tipos de danos causados às vítimas e os objetivos almejados pelos infratores. Neste intento, podemos classificar tais crimes como puros, mistos, comuns, próprios e impróprios.

De acordo com Schmidt, os crimes cibernéticos puros (também chamados de próprios) se referem a condutas ilícitas que têm como alvo principal o sistema de computador ou as informações contidas nele, seja por meio de danos físicos ou técnicos aos equipamentos e seus componentes, incluindo dados e sistemas. São exemplos dessa categoria as condutas previstas no art. 266, parágrafo primeiro (Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública), art. 313 A (Inserção de dados falsos em sistema de informações) e 313 B (Modificação ou alteração não autorizada de sistema de informações)**,** todos do Código Penal Brasileiro.

Já os delitos cibernéticos mistos são caracterizados pelo uso da internet ou de sistemas informáticos como condição essencial para a realização da conduta, embora o alvo do crime não seja necessariamente relacionado à informática, ou seja, o agente não tem como objetivo direto atacar o sistema de informática e seus componentes, porém, o uso da tecnologia é um instrumento indispensável para a consumação da ação criminosa. Podemos citar como exemplo o delito do art. 184, parágrafo terceiro, do CP (violação de direito autoral).

Por fim, ainda há os crimes cibernéticos comuns (impróprios) referem-se àqueles em que a internet é empregada meramente como uma ferramenta para a execução de um delito já definido pela legislação penal. Nesses casos, a Rede Mundial de Computadores é apenas mais um meio utilizado para a prática de uma conduta criminosa, como ocorre nos art. 155, parágrafo 4º e art. 171, parágrafo 2º, ambos do Código Penal.

Em suma, as classificações apresentadas fornecem uma estrutura crucial para compreender a diversidade e a complexidade das atividades criminosas no ambiente digital. Ao distingui-las conseguimos não apenas discernir suas características, mas também entender os modos de operação e os impactos sobre as vítimas e a sociedade.

3 COMPETÊNCIA PARA O PROCESSO E JULGAMENTO DOS CRIMES CIBERNÉTICOS

O Estado desempenha, por meio da jurisdição, a função de resolver litígios e restaurar a ordem e a tranquilidade na sociedade. A distribuição da jurisdição entre os diversos órgãos do Poder Judiciário é estabelecida por lei, através da atribuição de competências. Assim, a competência, quando definida com base na natureza do conflito a ser julgado, é conhecida como competência material. Já a competência funcional é aquela que determina quem tem o poder de julgar com base nas fases do processo, no objeto do juízo ou no grau de jurisdição.

No que diz respeito à competência material, três aspectos devem ser considerados para delimitar o exercício do poder jurisdicional: o território (ratione loci), a natureza da infração (ratione materiae) e a qualidade da pessoa do réu (ratione personae). Dessa forma, conforme estabelecido no artigo 69 do Código de Processo Penal (Brasil, 1941), a competência jurisdicional é determinada pelo local onde ocorreu a infração, pelo domicílio ou residência do réu, pela natureza da infração, pela distribuição, pela conexão ou continência, pela prevenção e pela prerrogativa de função.

De acordo com Matos (2014, p. 1):

> O grande desafio ao se trabalhar com o conceito de jurisdição e territorialidade no ambiente informático encontra-se na característica da globalização da rede, uma vez que nesta não existem limites territoriais, de forma que uma matéria publicada nela estará disponível no mundo inteiro. Assim, a consequência processual penal referente à jurisdição e à competência na internet se deve ao fato de que esta criou um espaço ilimitado e sem fronteiras.

Dessa forma, devido à amplitude do ambiente informático, a determinação da jurisdição competente para iniciar uma ação penal pode se apresentar como uma questão desafiadora. Tal problemática surge da complexidade de que os crimes cibernéticos, frequentemente, envolvem condutas realizadas à distância que produzem efeitos em múltiplos locais, podendo configurar, se a ação ou a consumação do delito ocorrer fora do território nacional, o chamado crime à distância (crime de espaço máximo). Se ambas as condutas, apesar de ocorrerem dentro do território nacional, se desenrolarem em comarcas distintas, configurar-se-á um crime plurilocal.

Conforme Souza (2023, p. 53), a definição da competência nos casos de crimes cibernéticos é uma questão complexa:

> Como se sabe, esse tipo de delinquência ocorre num ambiente imaterial, muito embora possa causar prejuízos materializáveis às vítimas no mundo fenomênico. Resultado jurídico e resultado naturalístico, muitas vezes, são indissociáveis e ocorrem no mesmo momento, o que leva à imediatidade capaz de colmatar as fases finais do iter criminis (execução-resultado-exaurimento), trazendo complexidade para definição da competência, exemplo disso é o que ocorre nos delitos de fraude eletrônica com a finalidade de produzir vantagem econômica para o autor da conduta.

Ademais, no que tange à possibilidade de alcance da jurisdição brasileira sobre os crimes cibernéticos à distância (resultado no Brasil e conduta no exterior ou vice-versa), devemos adotar a teoria da ubiquidade, prevista no artigo 6º do Código Penal, segundo a qual o local do crime é aquele onde ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir o resultado.

Já no que tange à competência territorial, existem outras duas teorias relevantes relacionadas ao local do crime. A primeira é a teoria do resultado, que considera competente para o julgamento o juízo da comarca ou seção judiciária onde o crime foi consumado, ou seja, onde ocorreu o resultado. A segunda é a teoria da atividade, que define a competência tomando por base o local onde foram praticados os atos executórios, ou seja, a conduta criminosa em si. Frise-se que no caso de crimes plurilocais (ação e resultado no território nacional) a competência se definirá pelo local onde o resultado danoso ocorreu.

Convém relembrar que nos casos de crimes transnacionais [se a conduta do agente ocorre fora do território nacional e os efeitos prejudiciais para a vítima são sentidos no território brasileiro (ou vice-versa)], a competência para o processo e julgamento caberá à Justiça Federal, conforme estipulado no art. 109, V, da Constituição Federal.

Acerca da competência, assim pacificou a Terceira Seção do Superior Tribunal de Justiça:

> EMENTA: CONFLITO NEGATIVO DE COMPETÊNCIA. PROCESSUAL PENAL. PUBLICAÇÃO DE PORNOGRAFIA ENVOLVENDO CRIANÇA OU ADOLESCENTE ATRAVÉS DA REDE MUNDIAL DE COMPUTADORES. ART. 241 DO ESTATUTO DA CRIANÇA E DO ADOLESCENTE. COMPETÊNCIA TERRITORIAL. CONSUMAÇÃO DO ILÍCITO. LOCAL DE ONDE EMANARAM AS IMAGENS PEDÓFILO-PORNOGRÁFICAS. 1 - A consumação do ilícito previsto no art. 241 do Estatuto da Criança e do Adolescente ocorre no ato de publicação das imagens pedófilo-pornográficas, sendo indiferente a localização do provedor de acesso à rede mundial de computadores onde tais imagens encontram-se armazenadas, ou a sua efetiva visualização pelos usuários. 2 - Conflito conhecido para declarar competente

> o Juízo da Vara Federal Criminal da Seção Judiciária de Santa Catarina. (STJ Processo CC 29886/SP CONFLITO DE COMPETENCIA 2000/0057047-8 Relator (a) Ministra MARIA THEREZA DE ASSIS MOURA (1131) Órgão Julgador S3 - TERCEIRA SEÇÃO Data do Julgamento 12/12/2007 Data da Publicação/Fonte DJ 01/02/2008 p. 427 RT vol. 871 p. 517) (Brasil, 2008).

Após estabelecermos a justiça competente (federal ou estadual), procedemos à definição do foro competente (comarca ou seção judiciária), analisando a viabilidade de se delimitar o local da consumação do delito.

Se for viável identificar o local onde a infração se consumou (lembrando que os crimes cibernéticos tensionam exatamente essa noção de espaço, já que podem produzir efeitos em vários locais ao mesmo tempo) ou onde foi praticado o último ato de execução (no caso de crime tentado), este será o foro competente, conforme disposto no artigo 70 do Código de Processo Penal: “A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução” (Brasil, 1941).

Quando restar dúvidas acerca do local da consumação do crime, seguir-se-á a regra do §3º do mesmo artigo: “Quando incerto o limite territorial entre duas ou mais jurisdições, ou quando incerta a jurisdição por ter sido a infração consumada ou tentada nas divisas de duas ou mais jurisdições, a competência firmar-se-á pela prevenção”.

Porém, quando não for possível determinar o local do crime, a competência de juízo se definirá pelo domicílio do réu, nos termos do art. 72 do Código de Processo Penal. Aqui vale trazer à lume a inovação criada pela Lei 14.155 de 2021, que definiu como foro competente para o julgamento dos crimes patrimoniais cibernéticos que se operam com transferência bancária o local de domicílio da vítima.

> CPP Art. 70.
> § 4º Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção (Incluído pela Lei nº 14.155, de 2021) (Brasil, 1941).

Portanto, diante da complexidade da jurisdição e competência no âmbito dos crimes cibernéticos, percebemos a necessidade de adaptar os conceitos jurídicos tradicionais aos desafios impostos pelo ambiente digital. Assim, a determinação da

competência jurisdicional para processar e julgar esses crimes torna-se uma tarefa desafiadora, especialmente devido à natureza globalizada da internet, que transcende fronteiras territoriais.

4 AUTORIA E MATERIALIDADE NOS CRIMES CIBERNÉTICOS

No universo dos crimes cibernéticos, um desafio primordial reside na determinação da autoria das infrações. Raramente o indivíduo que planeja cometer um delito utiliza sua identidade verdadeira, muitas vezes recorrendo ao anonimato ou até mesmo assumindo a identidade de terceiros por meio do uso indevido de credenciais pessoais. No mundo obscuro das redes de computadores, a identificação visual ou por meio de documentos é praticamente inviável; entretanto, é possível rastrear o endereço da máquina responsável pelo envio das informações à rede, conhecido como endereço IP.

De acordo com Burdova (2022, p. 1):

> Um endereço IP (endereço Internet Protocol) é uma série de números atribuídos a cada dispositivo conectado a uma rede de computadores ou à internet. Os endereços IP identificam e diferenciam os bilhões de dispositivos online, como computadores e telefones celulares, e ajudam esses dispositivos a se comunicarem entre si. [...] Os endereços IP garantem a transmissão de dados para o local certo. Da mesma forma que pessoas e empresas precisam de um endereço físico para enviar e receber cartas pelo correio, os dispositivos de internet precisam de um endereço digital para enviar e receber dados.

O endereço IP é uma identificação atribuída a todos os computadores conectados à Internet, apresentado no formato A.B.C.D, em que cada letra representa um número entre 0 e 255 (por exemplo, 223.109.7.38). Esta identificação é fundamental para rastrear atividades online. Para isso, é crucial a colaboração dos provedores de acesso, responsáveis por fornecer aos usuários os números de IP.

Assim, ao identificar o IP utilizado em atividades criminosas, é necessário solicitar ao provedor informações sobre o respectivo usuário. No entanto, muitos serviços de conexão utilizam IP’s dinâmicos, o que significa que os usuários recebem um IP diferente a cada conexão à Internet. Portanto, além do número de IP, é necessário obter a data, a hora e o fuso horário da atividade criminosa para uma investigação eficaz.

Segundo Schmidt (2015), cada endereço IP está associado a um provedor de acesso à internet. Existem sites de registro dedicados a identificar a empresa provedora de acesso responsável por cada IP e uma vez que ela é identificada, é possível solicitar informações sobre o cliente que utilizou esse IP em determinado momento.

É importante destacar a distinção entre "interceptação de dados telemáticos" e "quebra de sigilo dos dados de conexão e de usuário". Ainda sob a visão de Schmidt, a quebra do sigilo dos dados de conexão do usuário se refere à disponibilização inicial, pelas empresas, das informações sobre o IP utilizado e o horário (incluindo o fuso horário) de uma ação criminosa realizada em serviços de Internet, como redes sociais, contas de e-mail e programas de mensagens instantâneas. Posteriormente, são fornecidas informações sobre o usuário que utilizou aquele IP de um determinado provedor, ou seja, o suposto endereço físico onde o dispositivo com acesso à Internet estaria localizado durante a conduta criminosa.

Por outro lado, a interceptação de dados telemáticos refere-se ao recebimento pela Autoridade Policial de todos os acessos e conexões realizados pelo investigado na Internet. Essa prática é equiparada, em termos legais, à interceptação telefônica e deve ser realizada durante o Inquérito Policial, mediante autorização judicial conforme previsto na legislação vigente. Para tanto, é necessário que o Poder Judiciário e o Ministério Público sejam acionados por meio de uma representação para obter a autorização judicial.

Ademais, outro fator que dificulta a identificação do agente ao se falar de crimes cometidos em ambiente virtual são os chamados Proxy.

Resumidamente, um proxy é um serviço que atua como um intermediário entre o usuário e a internet, encaminhando todas as requisições do usuário para os sites que ele deseja acessar. Como resultado, o endereço IP registrado nas páginas visitadas é o do proxy, e não o do usuário. Isso ajuda a proteger a identidade do usuário na rede, dificultando o rastreamento de suas atividades e promovendo seu anonimato.

Resta evidente que os criminosos estão constantemente desenvolvendo métodos para ocultar seus crimes na internet, tornando-os quase impossíveis de rastrear.

Quanto à materialidade dos delitos cibernéticos, devemos observar que embora muitos deles não deixem vestígios relacionados com o objeto jurídico tutelado, há outros tantos que podem provocar mudanças, seja no próprio dispositivo informático violado, seja na coisa atingida através dos recursos que os dispositivos eletrônicos ligados à rede mundial de computadores franqueiam aos criminosos.

Assim é relevantíssimo observar o artigo 158 do Código de Processo Penal que define a indispensabilidade do exame de corpo delito.

As provas da materialidade dos crimes cibernéticos produzidas durante a investigação policial são chamadas de provas digitais ou *e-evidence*.

Conforme explica Rosa (2022, p. 1):

> A prova digital (espécie da prova eletrônica) é a obtida e/ou produzida em ambiente eletrônico digital, em que os dados (*de base, de tráfego e de conteúdo*), em geral, vulneráveis, intangíveis e frágeis, devem ser extraídos e tratados em observância às normas técnicas, observada a cadeia de custódia digital, sob pena de ineficácia probatória.

Ao falarmos de provas obtidas no meio informático, sabemos que é muito fácil apagar, perder ou modificar as evidências colhidas, além de que, elas podem se misturar com dados legítimos ou ilegítimos durante o processo, o que requer uma análise minuciosa por parte dos técnicos e peritos envolvidos na investigação criminal.

Na maioria dos casos, para a devida comprovação da materialidade do delito, torna-se imperioso realizar a interceptação do fluxo de comunicações efetuadas por meio de um computador. No entanto, como mencionado anteriormente, tais interceptações só podem ser realizadas mediante autorização judicial.

5 APONTAMENTOS GERAIS SOBRE O "*HASH*" COMO MEIO DE PROVA NOS CRIMES CIBERNÉTICOS

Considerando o momento de realização das provas periciais e a dificuldade ou impossibilidade de sua repetição na fase processual da *persecutio criminis*, é imprescindível garantir às partes a possibilidade de se certificar sobre quais materiais foram realmente objeto da diligência probatória e, eventualmente, a chance de submeter tal material à opinião de outros especialistas.

Assim, todas as provas materiais de um delito que sejam objeto de perícia devem ser submetidas a uma cadeia de custódia, que nada mais é do que uma série

de procedimentos realizados de forma sequencial com o objetivo de assegurar que tais evidências obtidas fora do ambiente processual sejam coletadas e preservadas sem sofrer alterações que possam comprometer o desenvolvimento do processo.

Mas como garantir o corpo de delito nos crimes cibernéticos? Oliveira (2023) esclarece que:

> Em relação aos crimes digitais, a integridade da cadeia de custódia é assegurada por *hashes*, algoritmos, que funcionam como a impressão digital de um arquivo. Se os *hashes* forem idênticos, entre a busca e uso posterior, reforça-se a ideia de preservação da cadeia de custódia. Por outro lado, se apontada a divergência entre os *hashes* da coleta com os de um uso posterior no curso da investigação ou mesmo no processo judicial, por exemplo, há indícios de quebra dessa cadeia de custódia.

No entender de Syozi (2022), o "*hash*" é uma técnica que possui o propósito fundamental de converter uma quantidade variável de dados em um valor de tamanho fixo, independentemente da quantidade de informações, através de um algoritmo matemático específico. Assim, essa função é capaz de transformar um arquivo, chave ou *string* (arquivo de localização) em um novo valor numérico ou alfabético, possibilitando verificar se houve alguma modificação no item desde o momento de sua criação até o momento da verificação.

Essa técnica é amplamente empregada na área de cibersegurança para garantir a integridade das informações, proporcionar assinaturas digitais e facilitar o acesso rápido a grandes conjuntos de dados, como em índices de tabelas em sistemas de desenvolvimento. Além disso, quando aplicados em cadeias de *hashes*, desempenham um papel crucial na obstacularização do acesso a ativos de dados por hackers, tornando a tarefa de descoberta de informações sensíveis mais difícil.

Neste contexto, o emprego de *hashes* para verificar a integridade das evidências digitais desempenha um papel crucial na manutenção da cadeia de custódia nos delitos cibernéticos, já que, como destacado por Vital, diante da responsabilidade do Estado em garantir a integridade e a confiabilidade das provas apresentadas, inclusive quando estas são de natureza digital, não é suficiente presumir a veracidade das evidências quando há indícios de descuido na coleta e no armazenamento dessas provas.

Corroborando a ideia antes explicitada, no dia 7 de fevereiro de 2023, o Superior Tribunal de Justiça (STJ) proferiu uma decisão pela sua 5ª Turma, abordando a questão da inadmissibilidade de provas digitais que não possuem registro

documental sobre os procedimentos adotados pela polícia para garantir a integridade, autenticidade e confiabilidade dos elementos informáticos.

> PENAL E PROCESSUAL PENAL. AGRAVO REGIMENTAL NO RECURSO ORDINÁRIO EM HABEAS CORPUS. OPERAÇÃO OPEN DOORS. FURTO, ORGANIZAÇÃO CRIMINOSA E LAVAGEM DE DINHEIRO. ACESSO A DOCUMENTOS DE COLABORAÇÃO PREMIADA. FALHA NA INSTRUÇÃO DO HABEAS CORPUS. CADEIA DE CUSTÓDIA. INOBSERVÂNCIA DOS PROCEDIMENTOS TÉCNICOS NECESSÁRIOS A GARANTIR A INTEGRIDADE DAS FONTES DE PROVA ARRECADADAS PELA POLÍCIA. FALTA DE DOCUMENTAÇÃO DOS ATOS REALIZADOS NO TRATAMENTO DA PROVA. CONFIABILIDADE COMPROMETIDA. PROVAS INADMISSÍVEIS, EM CONSEQUÊNCIA. AGRAVO REGIMENTAL PARCIALMENTE PROVIDO PARA PROVER TAMBÉM EM PARTE O RECURSO ORDINÁRIO. 1. O *habeas corpus* não foi adequadamente instruído para comprovar as alegações defensivas referentes ao acesso a documentos da colaboração premiada, o que impede o provimento do recurso no ponto. 2. A principal finalidade da cadeia de custódia é garantir que os vestígios deixados no mundo material por uma infração penal correspondem exatamente àqueles arrecadados pela polícia, examinados e apresentados em juízo. 3. Embora o específico regramento dos arts. 158-A a 158-F do CPP (introduzidos pela Lei 13.964/2019) não retroaja, a necessidade de preservar a cadeia de custódia não surgiu com eles. Afinal, a ideia de cadeia de custódia é logicamente indissociável do próprio conceito de corpo de delito, constante no CPP desde a redação original de seu art. 158. Por isso, mesmo para fatos anteriores a 2019, é necessário avaliar a preservação da cadeia de custódia. 4. A autoridade policial responsável pela apreensão de um computador (ou outro dispositivo de armazenamento de informações digitais) deve copiar integralmente (bit a bit) o conteúdo do dispositivo, gerando uma imagem dos dados: um arquivo que espelha e representa fielmente o conteúdo original. 5. Aplicando-se uma técnica de algoritmo hash, é possível obter uma assinatura única para cada arquivo, que teria um valor diferente caso um único bit de informação fosse alterado em alguma etapa da investigação, quando a fonte de prova já estivesse sob a custódia da polícia. Comparando as hashes calculadas nos momentos da coleta e da perícia (ou de sua repetição em juízo), é possível detectar se o conteúdo extraído do dispositivo foi modificado. 6. É ônus do Estado comprovar a integridade e confiabilidade das fontes de prova por ele apresentadas. É incabível, aqui, simplesmente presumir a veracidade das alegações estatais, quando descumpridos os procedimentos referentes à cadeia de custódia. No processo penal, a atividade do Estado é o objeto do controle de legalidade, e não o parâmetro do controle; isto é, cabe ao Judiciário controlar a atuação do Estado-acusação a partir do direito, e não a partir de uma autoproclamada confiança que o Estado-acusação deposita em si mesmo. 7. No caso dos autos, a polícia não documentou nenhum dos atos por ela praticados na arrecadação, armazenamento e análise dos computadores apreendidos durante o inquérito, nem se preocupou em apresentar garantias de que seu conteúdo permaneceu íntegro enquanto esteve sob a custódia policial. Como consequência, não há como assegurar que os dados informáticos periciados são íntegros e idênticos aos que existiam nos computadores do réu. 8. Pela quebra da cadeia de custódia, são inadmissíveis as provas extraídas dos computadores do acusado, bem como as provas delas derivadas, em aplicação analógica do art. 157, § 1º, do CPP. 9. Agravo regimental parcialmente provido, para prover também em parte o recurso ordinário em habeas corpus e declarar a inadmissibilidade das provas em questão. (BRASIL. Superior Tribunal de Justiça. AgRg no Recurso em Habeas Corpus nº 143.169-RJ (2021/0057395-6). Agravante R L S M (preso). Agravado:

> Ministério Público do Estado do Rio de Janeiro. Relator: Ministro Jesuíno Rissato. Brasília, 7 de fevereiro de 2023 (Brasil, 2023).

Em resumo, é importante destacar, com base no que foi mencionado, que o uso do *hash* desempenha um papel fundamental na preservação da cadeia de custódia, garantindo a integridade das provas já obtidas e contribuindo para o progresso adequado das investigações. Além disso, ao utilizar o *hash*, assegura-se que as evidências digitais permaneçam intactas e autênticas ao longo do processo, fortalecendo a confiabilidade do material apresentado perante as autoridades competentes.

6 CONCLUSÃO

Procuramos abordar de forma sintética e direta os aspectos mais relevantes sobre a modalidade criminosa que se desenvolveu com o uso comercial da internet, a partir do início da década de 1990 e se tornou ainda mais presente na vida dos brasileiros após a eclosão da pandemia de Covid-19, eis que pessoas com pouca literacia digital se viram obrigadas, num curto intervalo de tempo, a utilizar dispositivos conectados à rede mundial de computadores para praticamente todos os atos do seu dia a dia.

Sabemos que os desafios que se apresentam para elucidação destes delitos vão muito além da formação de um acervo teórico sobre suas formas de manifestação, sendo imprescindível uma pesquisa continuada a respeito das melhores técnicas de encontro de sua autoria e materialidade, bem como da garantia aos eventuais acusados dos direitos ao contraditório e ampla defesa.

Assim, procuramos trazer ao leitor nossas impressões sobre as melhores maneiras de garantir a certeza das evidências e a manutenção da cadeia de custódia, concluindo que o uso do “*hash*” é um procedimento bastante frutífero na garantia da manutenção da higidez probatória dos crimes cibernéticos.

Entendemos que o aumento dos crimes cibernéticos gera desafios a serem enfrentados, sendo crucial promover o "letramento digital" entre os usuários da internet, especialmente os idosos, que são mais suscetíveis a serem ludibriados pelas novas tecnologias.

Por outro lado, é igualmente importante aprimorar a capacitação das forças policiais, bem como o aprofundamento no conhecimento do entendimento judicial a respeito, uma vez que o combate a esse tipo de crime requer especialização e constante atualização diante da velocidade das mudanças tecnológicas.

REFERÊNCIAS

AVELAR, Michael Procopio. Classificação dos crimes no Direito Penal: resumo completo. **Estratégia**. São Paulo, 2019. Disponível em: https://www.estrategiaconcursos.com.br/blog/classificacao-dos-crimes/. Acesso em: 29 mar. 2024.

BIONI, Bruno Ricardo. **proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BRASIL. **Constituição da República Federativa do Brasil**: promulgada em 5 de outubro de 1988: atualizada até a Emenda Constitucional n° 131, de 03.10.2023. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 26 mar. 2024.

BRASIL**. Decreto-Lei nº 2.848, 7 dezembro 1940.** Código Penal. Rio de Janeiro, DF: Presidência da República,1940. Disponível em: https://www.jusbrasil.com.br/topicos/204961035/artigo-218c-do-decreto-lei-n-2848de-07-de-dezembro-de-1940. Acesso em: 26 mar. 2024.

BRASIL. **Lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Rio de Janeiro, DF: 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm. Acesso em: 26 mar. 2024.

BRASIL. Superior Tribunal de Justiça. **AgRg no Recurso em *Habeas Corpus*.** Penal e processual penal. Agravo regimental no recurso ordinário em habeas corpus. Operação open doors. Furto, organização criminosa e lavagem de dinheiro. Acesso a documentos de colaboração premiada. Falha na instrução do habeas corpus. Cadeia de custódia. Inobservância dos procedimentos técnicos necessários a garantir a integridade das fontes de prova arrecadadas pela polícia. Falta de documentação dos atos realizados no tratamento da prova. Confiabilidade comprometida. Provas inadmissíveis, em consequência. Agravo regimental parcialmente provido para prover também em parte o recurso ordinário AgRg nº 143.169-RJ (2021/0057395-6). Agravante R L S M (preso). Agravado: Ministério Público do Estado do Rio de Janeiro. Relator: Ministro Jesuíno Rissato. Brasília, 7 de fevereiro de 2023. Disponível em: https://www.conjur.com.br/wp-content/uploads/2023/09/stj-reconhece-quebra-cadeia-custodia.pdf. Acesso em: 28 abr. 2024.

BRASIL. Superior Tribunal de Justiça. **Conflito negativo de competência**. Processual penal. Publicação de pornografia envolvendo criança ou adolescente através da rede mundial de computadores. Art. 241 do estatuto da criança e do adolescente. Competência territorial. Consumação do ilícito. Local de onde emanaram as imagens pedófilo-pornográficas. Processo CC 29886/SP CONFLITO DE COMPETENCIA 2000/0057047-8 Relator (a) Ministra MARIA THEREZA DE ASSIS MOURA (1131) Órgão Julgador S3 - TERCEIRA SEÇÃO Data do Julgamento 12/12/2007 Data da Publicação/Fonte DJ 01/02/2008 p. 427 RT vol. 871 p. 517). Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=200000570478&dt_publicacao=01/02/2008. Acesso em: 01 out 2024.

BURDOVA, Carly. **O que é e como funciona um endereço IP?** Site AVG. Praga/Chéquia. 2022. Disponível em: https://www.avg.com/pt/signal/what-is-an-ip-address. Acesso em: 31/03/2024.

CARDOSO, Wellington Clayton dos Santos. **Evolução tecnológica no direito penal e crimes cibernéticos.** Belo Horizonte, 2023. Disponível em: file:///C:/Users/anaef/Downloads/CENTRO%20UNIVERSITA%CC%81RIO%20DE%20BELO%20HORIZONTE%20-%20(UNIBH).pdf. Acesso em: 25/03/2023.

HUOSEL FILHO, Valmar. Considerado o ‘crime da moda’, estelionato digital cresce no Brasil. **Revista Veja**. São Paulo. 2023. Disponível em: https://veja.abril.com.br/brasil/considerado-o-crime-da-moda-estelionato-digital-cresce-no-brasil. Acesso em: 02 abr. 2024.

MATOS, Mariana Maria. A definição da competência nos crimes virtuais. **Jusbrasil**. São Paulo, 2014. Disponível em: https://www.jusbrasil.com.br/artigos/a-definicao-da-competencia-nos-crimes-virtuais/119753666. Acesso em: 26/03/2024.

MOREIRA, Paulo Roberto Silvério. Estelionato praticado por meio da internet: Uma visão acerca dos crimes digitais. **Migalhas**. São Paulo, 2022. Disponível em: https://www.migalhas.com.br/depeso/359821/estelionato-praticado-por-meio-da-internet. Acesso em: 02 abr. 2024.

OLIVEIRA, Marcelo Ribeiro de. Cadeia de custódia digital: cuidados na preservação e especificação da metodologia. **Consultor Jurídico**. Brasília, DF, 2023. Disponível em: https://www.conjur.com.br/2023-mar-23/marcelo-oliveira-cadeia-custodia-digital-cuidados-metodo/#:~:text=A%20cadeia%20de%20cust%C3%B3dia%20%C3%A9,impress%C3%A3o%20digital%20de%20um%20arquivo. Acesso em: 15 abr. 2024.

ROCHA, Rafael. Saiba o que é o Crime de Estelionato. **Jusbrasil**. Goiás, 2018. Disponível em: https://www.jusbrasil.com.br/artigos/saiba-o-que-e-o-crime-de-estelionato/628482441. Acesso em: 02 abr. 2024.

ROSA, Alexandre Morais da. Limite penal: o *"print screen"* é insuficiente à materialidade nos crimes digitais**. Consultor Jurídico**. Santa Catarina, 2022. Disponível em: https://www.conjur.com.br/2022-jun-17/limite-penal-print-screen-materialidade-crimes

digitais/#:~:text=A%20materialidade%20%C3%A9%20indispens%C3%A1vel%20nos,de%20validade%20e%20de%20efic%C3%A1cia. Acesso em: 31 abr. 2024.

SCHMIDT, Guilherme. Crimes cibernéticos. **Jusbrasil**. São Paulo, 2015. Disponível em: https://www.jusbrasil.com.br/artigos/crimes-ciberneticos/149726370#:~:text=Crimes%20Cibern%C3%A9ticos%20Puros%2C%20Mistos%20e%20Comuns,Crimes%20cibern%C3%A9ticos%20puros&text=%C3%89%20aqui%20que%20entram%20as,ou%20prejudicar%20servidores%20e%20sistemas. Acesso em: 25 mar. 2024.

SYOZI, Ricardo. O que é um hash? **Tecnoblog**. São Paulo, 2022. Disponível em: https://tecnoblog.net/responde/o-que-e-um-hash/. Acesso em: 15 abr. 2024.

SOUZA, Wesley Wadin Passos Ferreira de. A Convenção de Budapeste e seus reflexos sobre a competência para o processo e julgamento dos crimes cibernéticos no Brasil. **Revista Judicial Brasileira**, ed. especial. Direito Digital, Brasília, DF, 2023. Disponível em: https://revistadaenfam.emnuvens.com.br/renfam/issue/view/17/8. Acesso em: 25 mar. 2024.

VITAL, Danilo. Furtos eletrônicos: STJ reconhece quebra da cadeia de custódia e anula provas digitais. **Consultor Jurídico**. Brasília, DF, 2023. Disponível em: https://www.conjur.com.br/2023-mar-06/stj-reconhece-quebra-cadeia-custodia-anula-provas-digitais/. Acesso em: 15 abr. 2024.