UNICEPLAC

Centro Universitário do Planalto Central Apparecido dos Santos - UNICEPLAC

Curso de Direito

Trabalho de Conclusão de Curso

As dificuldades na colheita de elementos de autoria e materalidade delitiva dos Crimes Cibernéticos

Gama-DF

2021

LUDMILLA GONÇALO DA SILVA SODRÉ

Dificuldades na colheita de elementos de autoria e materalidade delitiva dos Crimes Cibernéticos

Artigo apresentado como requisito para conclusão do curso de Bacharelado em Direito pelo Centro Universitário do Planalto Central Apparecido dos Santos – Uniceplac.

Orientador: Danilo Rinaldi dos Santos Junior

Gama-DF

2021

LUDMILLA GONÇALO DA SILVA SODRÉ

As dificuldades na colheita de elementos de autoria e materalidade delitiva dos Crimes Cibernéticos

Artigo apresentado como requisito para conclusão do curso de Bacharelado em Direito pelo Centro Universitário do Planalto Central Apparecido dos Santos – Uniceplac.

Gama-DF, 26 de novembro de 2021.

Banca Examinadora

Prof. Danilo Rinaldi dos Santos Junior
Orientador

Prof. Caroline Lima Ferraz
Examinador

Prof. Risoleide de Souza Nascimento
Examinador

As dificuldades na colheita de elementos de autoria e materalidade delitiva dos Crimes Cibernéticos

Ludmilla Gonçalo da Silva Sodré

Resumo
Com o crescente e constante avanço tecnológico, a utilização da internet se torna mais recorrente. Ao lado do uso comum e rotineiro do dos meios de comunicação também surte o uso anormal, com vistas a obtenção de resultados ilícitos. O presente estudo busca analisar os crimes cibernéticos acometidos pelo uso abusivo dos recursos tecnológicos que giram em torno da internet, compreender a legislação aplicada e os crimes mais comuns nessa modalidade, e por fim analisar as dificuldades de apuração e punição aos autores que se valem de falhas sistemáticas para o acometimento de crimes

Palavras-chave: 1. Crimes cibernéticos. 2. Autoria e materialidade delitiva.

Abstract:
With the constant and growing technological advancement, the use of the internet becomes more recurrent. In addition to the common and routine use of the media, there is also abnormal use, with a view to obtaining illicit results. This study seeks to analyze cyber crimes affected by the abusive use of technological resources that revolve around the internet, understand the applied legislation and the most common crimes in this modality, and finally analyze the difficulties of investigation and punishment for perpetrators who use systematic failures to commit crimes

Keywords: 1. Cyber crimes. 2. Criminal authorship and materiality.

1. INTRODUÇÃO

A concepção inicial de internet deu início no ano de 1969 nos Estados Unidos, e teve como propósito auxiliar os militares na Guerra Fria. Com o fim da Guerra, a internet se estendeu também para outros escopos, principalmente no âmbito social, a qual incentivou a utilização do primeiro computador digital, também chamado de ENIAC, criado para a realização de cálculo de tabelas balísticas (SANTOS; MARTINS; TYBUCSH, 2014).

Com grandes mudanças, a evolução da internet foi acontecendo gradativamente, se adequando as necessidades do ser humano, tornando-se cada vez mais eficaz e simplificada. Inovações com máquinas tecnológicas passaram a aderir proporções cada vez menores, de modo que fosse possível portar, como o smartphone. A evolução da internet se dá de maneira constante, facilita a vida cotidiana de um indivíduo sem que ele precise se deslocar, tendo acesso remoto em qualquer site na palma de sua mão (LINS, 2013).

Hodiernamente, com avanço tecnológico acesso há uma maior comodidade aos usuários o amplo acesso aos meios de comunicação, a contas bancárias, pagamentos de boletos, compras em geral, por meio de um smartphone, o que torna o indivíduo cada vez mais dependente, e consequentemente gera mais riscos a sua segurança e dignidade.

Não é difícil identificar inúmeros casos da utilização dos meios cibernéticos para a promoção de atos ilícitos, isto porque ante ao avanço tecnológico, aqueles que conhecem suas fragilidades podem se valer de artifícios que dificultem a identificação da autoria e materialidade delitiva. Nesse aspecto, há avanços legislativos e procedimentais que buscam efetivar o cumprimento da demanda punitiva frente a lesão de bens jurídicos tutelados pelo Estado, entretanto, diante do dinamismo dos avanços tecnológicos, há uma necessidade maior de adequação ao plano fático.

Nesse sentido, o presente trabalho é fruto de uma pesquisa bibliográfica, utilizando do método indutivo, que busca verificar o acometimento de crime cibernéticos, acometidos pelo uso abusivo dos recursos tecnológicos que giram em torno da internet, sua legislação e os crimes mais comuns nessa modalidade, e por fim analisar as dificuldades de apuração e punição aos autores que se valem de falhas sistemáticas para o acometimento de crimes.

2. DA LEGISLAÇÃO

Inicialmente, o Código Penal Brasileiro em seu art. 1º enfatiza que não existe uma conduta criminosa se a lei não a definir como crime. Outrossim, corroborando com isso Rogério Greco discorre que a lei é como fonte primária do Direito Penal, uma vez que ao dispor sobre condutas e cominar penas à estas, busca-se proteger determinados bens jurídicos, de maneira que, tão somente àquelas condutas descritas como crimes podem ensejar as penas correspondentes. Sendo assim, aquilo que não for descrito como crime não será ilícito ao direito penal (GRECO, 2019).

Fernando Capez corroborando com esse raciocínio, aduz que haverá crime quando houver previsão legal daquela conduta praticada, e, pela teoria de Binding, preceitua-se que as normas penais incriminadoras são descritas e não proibitivas. Com isso conclui que a prática de um crime não é maneira antagônica à lei, mas de acordo com ela, pois os delitos estão pormenorizadamente descritos nos diplomas legais, sendo denominados tipos penais. Ou seja, a lei não proíbe o crime, mas defini-o enquanto delito, propiciando ao agente tanto o conhecimento dos fatos tido como tal, como as penalidades que pode sofrer com a prática daquela atividade delituosa. (CAPEZ, 2021)

Nesse sentido, por se tratar de um assunto relativamente recente, os crimes cibernéticos estão descritos tanto no Código Penal quanto em legislações próprias. Insta mencionar que existem diversas terminologias utilizadas por doutrinadores para conceituar o crime cibernético, como: crimes virtuais, crimes digitais, crimes informáticos, e outros. No entanto, assevera Patrícia Santos da Silva:

> [...]que não há uma nomenclatura sedimentada pelos doutrinadores acerca do conceito de crime cibernético. De uma forma ou de outra o que muda é só o nome atribuído a esses crimes, posto que devem ser observados o uso de dispositivos informáticos, a rede de transmissão de dados para delinquir, o bem jurídico lesado, e ainda deve a conduta ser típica, antijurídica e culpável. (SILVA, 2015)

Posto isto, conceituando com uma nomenclatura mais holista, o Crime Cibernético engloba diferentes condutas delitivas praticadas com o uso de aparelhos eletrônicos, tratando-se de condutas ilícitas realizadas por qualquer tipo de dispositivo tecnológico, como smartfones, computadores e afins, por entender-se que as realizações das condutas são dadas em um ambiente virtual, com necessário acesso aos meios digitais decorrentes da internet. Sob tal viés, Ivette Senise

Ferreira, infere que:

> As várias possibilidades de ação criminosa na área informática, assim entendida em seu sentido lato, abrangendo todas as tecnologias da informação, do processamento e da transmissão de dados, originaram uma forma de criminalidade que, apesar da diversidade de suas classificações, pode ser identificada pelo seu objeto ou pelos meios de atuação, os quais fornecem um denominador comum, embora com diferentes denominações nos vários países ou nos diferentes autores. (FERREIRA 2001, p. 208)

Destarte, Antônio Lima enfatiza que são crimes de acesso não autorizado pelo sistema informático, no qual se pode citar como exemplo as interceptações de comunicação, modificações de dados, infrações de direitos autorais, incitação ao ódio, descriminação, escárnio religioso, difusão de pornografia infantil, terrorismo e afins. Sendo, ainda, importante destacar que a denominação dos delitos deve ser feita em consonância com bem jurídico protegido após a averiguação e constatado a veracidade se é crime virtual, aplica-se o tipo penal correspondente àquela prática delituosa, considerando o bem jurídico tutelado (LIMA, 2014)

De pronto, a primeira legislação específica a tratar dos crimes virtuais se dá pela Lei 12.737/2012, denominada Lei Carolina Dieckmann, que surgiu em março de 2012. A atriz Carolina Dieckmann foi vítima de crime cibernético quando teve suas fotos íntimas foram copiadas após uma invasão em seu dispositivo. O crime se deu por um quando a Atriz inocentemente abriu um e-mail que acreditava se fonte segura. Pelo engajamento da atriz em relação à este tipo de delito e seu anseio como vítima, a lei passou a ter su nome. (SANTOS *et al*, 2014)

Com isso, o projeto de lei tramitou de forma mais célere e tornou-se Lei em 30 de novembro de 2012, tendo como objetivo tipificar os crimes informáticos, uma vez que até então não havia lei específica tipificando especificamente este tipo de crime, o que muitas vezes levava os agentes anteriormente a serem tipificados por outros crimes do código penal. A referida lei também determinou a estruturação e especialização das policias judiciárias com fito de combater esses delitos, modificou a Lei 7.716, Lei de Crime Racial, através do inciso II do § 3º de seu artigo 20, com intento de interromper transmissões radiofônicas, televisivas, eletrônicas ou publicações por qualquer meio da prática, indução ou incitação de discriminação de raça, cor, etnia, religião ou procedência nacional.

Destarte, o Decreto 7.962, de 2013 regulamentou o Código de Defesa do Consumidor em relação ao Comércio Eletrônico (e-commerce) e as chamadas

vendas on-line, visando proteger o consumidor de insatisfações com o produto adquirido e possíveis fraudes. Portal do conhecimento (2019). Outrossim, ficou imposto aos fornecedores que disponibilizassem no sítio eletrônico, em local de fácil acessibilidade e visibilidade o nome empresarial e o número de registro CNPJ, bem como o fornecimento de endereço físico e eletrônico ao consumidor. Ainda, as regras se estenderam para ofertas nos sites de compra coletiva e determinou a apresentação de sumário do contrato ao consumidor antes da celebração do mesmo, tornando, também, o fornecedor responsável pela informação dos meios para o exercício do direito de arrependimento da compra pelo consumidor". (TJRJ, 2019)

Outro momento de grande relevância foi o Marco Civil da Internet, Lei 12.965/2014, que trouxe diversas inovações, dentre elas está: Proteção da privacidade e proteção dos dados pessoais, vedada a utilização comercial de dados pessoais dos internautas, sem consentimento expresso do usuário e outras.

O marco civil foi dividido em duas partes, dos princípios norteadores do projeto e os princípios fundamentais; e a fase de concretização de tais princípios. Num prisma geral, buscou-se promover a liberdade de expressão, o direito ao acesso à internet, a privacidade na utilização do serviço, a neutralidade da rede, os limites à responsabilidade dos intermediários e a defesa da abertura da rede, como meio para a inovação (LEMOS; LEITE, 2014), conforme:

> Com isso, ao dar um passo no sentido de regulamentar essa questão o Marco Civil atende a dois princípios importantes. O primeiro de fortalecer o princípio da liberdade de expressão, protegendo em alguma medida os intermediários da informação. Em segundo lugar, impulsiona a inovação local, na medida em que permite a jovens empreendedores brasileiros saberem de antemão os limites da sua responsabilidade, gerando previsibilidade e alavancando o surgimento de novos serviços baseados no país (LEMOS; LEITE, 2014)

Contou-se ainda com a participação popular através de debates abertos e coletivos, tendo sido o texto legal sido posto em outras plataformas online para visualizar-se o debate público acerca do tema. O projeto fundou-se em três pilares: garantia da neutralidade da rede, a garantia da liberdade de expressão e comunicação, e a privacidade dos usuários e de seus dados; tais pilares buscaram de maneira essencial à proteção aos dados pessoais disponibilizados, a integração com os provedores que recebem os dados de maneira a garantir e assegurar os direitos dos usuários dos serviços (AKCHAR, 2017)

Já em 2016 houve a publicação de um Decreto 8.771 que regulamentou

pontos do Marco Civil como a neutralidade da rede e a proteção de registros de acesso e dados pessoais. Em 2018 foi publicada a lei a Lei nº 13.709 Geral de Proteção de Dados Pessoais (LGPD), com vigência total prevista para dois anos afrente, que alterou a lei 12.965/2014, passando a dispor sobre o tratamento dos dados pessoais, inclusive no meio digital, com objetivo de protege-los, como também a liberdade e privacidade dos usuários de serviço, inclusive eletrônicos.

Buscou-se então um melhor cenário de segurança jurídica, uniformizando as normas e práticas adotadas, buscando promover a proteção de forma igual dentro e fora do país, aos dados pessoais de todos os cidadãos que estejam no Brasil. Daí definiu-se como dados pessoais todas as informações que possam identificar, de forma direta ou indireta, qualquer indivíduo, como: CPF, gênero, data e local de nascimento, telefone, endereço residencial, entre outros (SERPRO, 2018)

Estabeleceu-se, ainda o órgão responsável pela fiscalização da aplicação da LGPD, sendo determinada à Autoridade Nacional de Proteção de Dados Pessoais (ANPD), sendo responsável pela fiscalização e aplicação de mutas, bem como regular a como será aplicada a lei. Consequentemente, a lei determinou a responsabilidade do administrador da base de dados pessoais o dever de elaborar normas de administração dos dados, cumprir determinada medidas de segurança a garantir o não vazamento dos dados, e ocorrendo, o dever de noticiar à todos os usuários. E assim, determinou-se que as falhas de segurança podem gerar multas de até 2% do faturamento anual da organização, até o limite de 50 milhões por infração, sendo analisado o grau da falha pela autoridade competente (SERPRO, 2018)

Ademais em razão da necessidade de lei específica com penalidades mais duras, foi sancionada a Lei 14.155, de 2021, alterando-se o Código Penal, Decreto-Lei 2.848/1040, agravando as penas dos crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet, e alterando o Código de Processo Penal, Decreto-Lei nº 3.689/4, de forma a definir a competência em modalidades de estelionato.

Em que pesem tais contribuições, SCHAUN (2018) infere que a ecolução legislativa é timida, de maneira que não acompanha de maneira inquívoca o dinamismo da tecnologia virtual, assim, mesmo havendo uma lista extensa de crimes cibernéticos, estes são pouco especificados, de maneira que carecem um perfeito adequamento típico.

3. DOS CRIMES CIBERNÉTICOS

Os crimes virtuais possuem alta popularidade, uma vez que na maioria das hipóteses para seu cometimento não há necessidade que o agente possua específicos conhecimentos técnicos do uso de computadores, sendo necessário tão somente a vontade destinada à uma finalidade, valendo-se da internet como meio ou o próprio bem jurídico a ser lesado.

Diante do exponencial crescimento do uso da tecnologia da informação, a rede mundial de computadores toma uma proporção enorme no cotidiano de qualquer indivíduo. Nesse prisma, a internet e seus meios fazem parte da vida em sociedade, uma vez que evidenciam um meio de comunicação, de comércio, de obtenção de pesquisas, pagamento de contas, promoção da educação e afins. Nesse sentido, a utilização da internet evidencia um ato cotidiano, que tanto pode ser utilizado para suas finalidades iniciais, quanto para pratica de atos delituosos, denominados crimes cibernéticos, virtuais ou de informática (DORIGON; SOARES, 2017).

A primeira classificação que se verifica é realizada por Augusto Rossini, que os divide como próprios, impróprios, mistos, mediato ou indireto. Definindo como crimes cibernéticos próprios aqueles em que o bem juridico protegido pela norma penal é a inviolabilidade das informações automatizadas. Quando não há ofensa ao bem jurídico da inviolabilidade da informação automatizada serão denominadas de crimes informáticos impróprios, sendo o computador usado como instrumento do crime (VIANNA; MACHADO, 2013).

Já os crimes informáticos mistos são os crimes de natureza mais complexa, aonde a norma jurídica tutela bem jurídico de natureza diversa, classificado como *suis generis* em razão importância do bem jurídico protegido ser inviolabilidade dos dados informáticos como bem diverso. Por fim, os crimes mediatos ou diretos, estão conceituados como delito-fim não informático, que herdou esta característica do delito-meio informático realizado para possibilitar a sua consumação (ROSSINI, 2004). Há ainda classificação idealizada que diversifica que crimes de informática, sendo eles: praticados por meio de computador, quando este é o instrumento idealizado à realização da prática criminosa; e os crimes contra o sistema informático em sí, sendo aqueles em que a finalidade do delito se dá contra os

dados informáticos. (MARRA, 2019)

Já a origem dos crimes cibernéticos se deu após sua a criação da internet, em meados de 1980 atinge um aumento frente a figura dos hackers, usuários que detinham certa inteligência tecnológica e utilizavam destes conhecimentos para o acometimento de crimes cibernéticos, como a invasão e furto de softwares. Invasão de sistemas, pirataria, pedofilia e afins (CARNEIRO, 2012).

São exemplos os crimes que podem ser cometidos por meio virtual, conforme dispostos no código penal brasileiro: Calúnia (art. 138), Difamação (art. 139), Injúria (art. 140), Ameaça (art. 147, Furto (art. 155), Dano (art. 163), Apropriação indébita (art. 168); Estelionato (art. 171), Violação ao direito autoral (art. 184), entre outros. Já na legislação especial, também são encontrados os crimes: Pedofilia (art. 240 e 241), e Pornografia infantil (art. 234) ambos da Lei nº 8.069/90 – Estatuto da Criança e do Adolescente; Crime contra a propriedade industrial (art. 183 e ss.) da Lei nº 9.279/96 ; Interceptação de comunicações de informática ou Interceptação de E-mail Comercial ou Pessoal (art. 10) da Lei nº 9.296/96; Crimes contra software – “Pirataria” (art. 12) da Lei nº 9.609/98, dentre outros tipos penais diversos no ordenamento jurídico.

Em tese, são diversas hipóteses de crimes a serem cometidos e alguns chamam mais a atenção, são as hipóteses do estelionato (art. 171, CP) realizado de maneira remota, em que os agentes criam falsos sites e induzem as vítimas à acreditarem na veracidade de tais sítios, fazendo com que exponham diversos dados sigilosos, que são utilizados para realização de compras na internet, à venda de tais dados ou ainda a utilização destas informações para o acometimento de outros crimes (MARTINS, 2020; SANTOS *et al*, 2014).

Doutro lado, também tem se intencionado os crimes de extorsão (art. 159, CP) que também possui diversas modalidades de realização, sendo seu *modus operandi* livre, e ocorre por meio da obtenção de dados sigilosos da vítima, fotos ou demais dados pela utilização de programas destinados a esta finalidade, que permite o acesso do computador e celular da vítima, daí sequestram tais dados e ameaçam a vítima de expô-los ou ainda apaga-los frente a uma exigência de pagamento. Há ainda o crime de sextorção, ou chantagem sexual, pela qual os autores de tais crimes obtém vídeos e fotos íntimas da vítima e ameaçam-na a sua divulgação em redes sociais, buscando que um pagamento em dinheiro (SANTOS, 2020).

Surge, ainda, a chamada ciberpedofilia (art. 240,241 e 234 ambos da Lei nº 8.069/90), crime sexual praticado contra crianças e adolescentes por intermédio da internet. Nestas hipóteses, os ciberpedófilos utilizam de diversos mecanismos para atrair as vítimas, valendo-se de falsos perfis na internet, e utilização de uma linguagem infantil ou condizente ao adolescente, buscando criar vínculos de confiança para chantagear emocionalmente as vítimas e a partir disso conseguir conteúdo pornográfico, uma espécie de estupro virtual (MARRA, 2019).

Não se olvidando dos crimes contra a honra, que possuem grande destaque a calúnia e difamação, são conhecidos também como cyberbullying ocorrem de maneira hodierna nos meios eletrônicos e são crimes que buscam injuriar, difamar intimidar e ofender alguém lhe causando desconforto por inúmeros fatores de maneira intencional e repetidamente, se dá normalmente em redes sociais e o dolo é direcionado à uma pessoa ou grupo(MARTINS, 2020).

Doutro lado do cyberbullying, há também o crime de ameaça, que demonstra maior violência no meio que se propaga, pois se ameaça-se a pessoa de mal injusto, como de morte à pessoa, ou seus entes em decorrência de quaisquer desentendimentos.

3.2. Do agravamento dos crimes cibernéticos em tempos de pandemia

Os crimes cibernéticos sempre foram comuns no Brasil e vieram evoluindo juntamente com o avanço e as mudanças constantes da tecnologia, todavia, durante a pandemia do COVID 19, esses delitos alcançaram o maior índice de ocorrências. Em uma notícia veiculada pelo Correio Brasilense, consignou-se que aproveitando-se da crise sanitária, foram intensificaram as práticas delituosas no ano de 2020, uma vez houve registro de 17.843 casos, aumento de 87,1% em comparação com 2019. Em relação a estelionatos, o crescimento foi de 209%”. (CORREIO BRASILIENSE, 2021) Vê-se uma adaptação dos criminosos à pratica de ilícitos desenvolvidos por meio virtual, tanto pela comodidade da ação, quanto a possibilidade do anonimato. Corrobrando tal entendimento:

> De fato, o isolamento social foi capaz de reduzir significativamente a prática de roubos e furtos nas cidades brasileiras, como consequência do zelar da população, ao preferir a segurança do ambiente domiciliar. No entanto, estas mesmas circunstâncias, serviram para a desenvoltura de crimes cibernéticos cometidos por Crackers. (MARTINS, 2020)

Isso ocorre devido facilidade e fragilidade da sociedade na utilização dos

mecanismos que a internet proporciona para resolução de questões básicas pessoais, como pagamentos de contas, compras sejam elas de grande ou pequeno valor, assinaturas virtuais, transferências bancárias sem pagamento de taxas, dentre outras milhares de operações virtuais. (VIANNA; MACHADO, 2013; SANTOS *et al*, 2014)

Destarte, Rodrigo Fogagnolo, promotor e coordenador Núcleo de Combate a Crimes Cibernéticos (Ncyber) do MPDFT, afirma em entrevista que têm-se criado novas formas de agir durante a pandemia para atingir mais vítimas, sendo o aplicativo Whatsapp um dos meios mais utilizados, dado sua facilidade de uso e comodidade por parte dos usuários. Afirma Fagnolo que são através de mensagens enviadas por criminoso para fornecimento de um PIN que criminoso conseguem prosperar em suas práticas.

Ademais, enfatiza o delegado Giancarlos Zuliani, titular da Delegacia Especial de Repressão aos Crimes Cibernético que devido muitas pessoas precisarem ficar em casa para evitar a contaminação do vírus, facilitou a atuação dos estelionatários para chegarem ao resultado pretendido. E conclui, “As pessoas estão utilizando mais a internet, seja para comprar, seja usar as redes sociais ou conversar por meio dos aplicativos de mensagens. Consequentemente, elas ficam mais sujeitas a esse tipo de crime” (CORREIO BRASILIENSE, 2021).

O isolamento social em si foi responsável por reduzir significativamente a pratica dos crimes de roubo e furto uma vez que a impossibilidade do acometimento de tais crimes está veiculada a uma presença física tanto do autor quanto da vítima. Por outro lado, infelizmente, agravou-se o acometimento de crimes virtuais, os quais são pautados pela desnecessidade da presença física dos agentes, isso decorre duma necessidade massiva da utilização das redes de comunicação para realização de diversos serviços, afazeres e afins, surgindo uma maior adaptação dos agentes à utilização da internet como meio a obtenção de diversos resultados criminosos (PEREIRA *et al,* 2021). Nesse sentido:

> [...] as formas de crimes vêm se desenvolvendo tal qual as tecnologias, assim sendo possíveis formas de ilícitos antes não imaginadas, mas que já passam a ser alvo de observação do Estado. Tanto a concepção sociológica como econômica já havia previsto o aumento de crimes em épocas conturbadas como a que vivenciamos atualmente, porém devido a enorme importância que os dispositivos eletrônicos possuem em nosso cotidiano, é percebível o nosso despreparo referente a segurança nesses meios ainda recentes.

Daí há a demonstração de um efetivo efeito colateral dos tempos de

isolamento social atrelado à crise econômica; sendo, então, o crime em seus infinitos meios, um sintoma nítido das consequências sociais de tempos conturbados. Doutro lado, há a necessidade de políticas públicas aptas a prevenir o acometimento de tais crimes, de maneira a instruir as possíveis vítimas sobre os crimes que estão sendo aplicados e os meios e mecanismos aptos a evitar a consumação do delito (COUTINHO, 2021).

4. A DIFICULDADE DE COLHEITA DE ELEMENTOS DE AUTORIA E MATERIALIDADE DELITIVA

No processo penal, a reconstituição do fato delituoso enseja obtenção de provas aptas a ensejar um juízo de culpa ao agente, sendo ela imprescindível a formação da convicção do juízo da existência ou não do fato alegado. Nesse sentido, a prova do fato e da autoria é fundamental ao exercídio da demanda punitiva. Nesse sentido, Fernando Capez (2021) leciona ser a prova o meio mais importante da ciência processual, isto porque se verifica que a prova constitui o alicerce processual pela qual será vinculado a culpa ou inocência do agente, sendo a verificação da idoneidade e validade da prova para obtençaõ do resultado útil do processo essencial ao devido processo legal.

Há, ainda uma diferenciação singela de meio de prova e meio de obtenção de prova, que deve ser observada, conforme preleciona Aury Lopes Jr:

> a) Meio de prova: é o meio através do qual se oferece ao juiz meios de conhecimento, de formação da história do crime, cujos resultados probatórios podem ser utilizados diretamente na decisão. São exemplos de meios de prova: a prova testemunhal, os documentos, as perícias etc.
> b) Meio de obtenção de prova: ou mezzi di ricerca della prova como denominam os italianos, são instrumentos que permitem obter-se, chegar-se à prova. Não é propriamente “a prova”, senão meios de obtenção. [...] que os meios de obtenção de provas não são por si fontes de conhecimento, mas servem para adquirir coisas materiais, traços ou declarações dotadas de força probatória, e que também podem ter como destinatários a polícia judiciária. Exemplos: delação premiada, buscas e apreensões, interceptações telefônicas etc. Não são propriamente provas, mas caminhos para chegar-se à prova.

Nesse interim, todos os fatos que não forem notórios evidentes ou que gozem de presunções legais devem ser corroborados no processo, sendo comprovado/provados pelo Estado acusador. A prova ainda deve ser lícita formal e materialmente, sob pena de desentranhada dos autos do processo, uma vez que afronta diretamente a Constituição Federal; deve, ainda, ter relação com o processo,

sendo um meio de esclarecimento da controvérsia (CAPEZ, 2021).

Ainda que o direito tutele, legislativamente, as práticas ilícitas que se dão pelo meio informático ou contra ele, e, há ainda muito a se progredir no meio tecnológico para se garantir e proporcionar a tutela jurisdicional. A dificuldade em apurar essas penalidades se dá pela falta de materialidade delitiva, que torna o trabalho investigativo complexo, uma vez que é possível o autor do crime executá-lo em um Estado da Federação, ou até em outro país, e a consumação de ser em qualquer lugar, ainda, podendo utilizar-se de meios que garantam seu anonimato.

Quer dizer, os crimes cibernéticos se dão de forma livre, sempre havendo inovações espetaculares para sua prática, que correm junto ao avanço tecnológico. E, assim sendo, pela facilidade de perpetuar qualquer conduta por meio tecnológico, inúmeros autores se revelam com aptos à tais atos, uma vez que podem se valer da dificuldade de apuração de tais crimes, do possível anonimato e afins, conforme:

> a mesma Internet que representa avanços tecnológicos na comunicação, na informação, na ciência, no comércio, é também aquela que difunde uma noção equivocada de impunidade, seja pelo referido anonimato, seja pela dificuldade no rastreamento do autor, ou ainda, seja pela dificuldade de aplicação da legislação em vigor (MARRA, 2019)

Dos maiores problemas enfrentados hoje em matéria de crimes cibernéticos de dá na dificuldade de angariar meios aptos a provar os indícios mínimos de autoria e materialidade delitiva pois há diversas possibilidades de qualquer um utilizar-se do anonimato no uso da internet, à alteração dos endereços eletrônicos, alteração do IP e o fácil desaparecimento de provas.

Nesse prisma, um dos problemas visualizados é a carência de colaboração e comunicação das autoridades competentes às vítimas desses crimes, tornando incerta o acometimento dos fatos delituosos. (SANTOS *et al*, 2014)

O dinamismo da informação e da tecnologia são elementos que contribuem à maior dificuldade das investigações referentes aos crimes virtuais e acompanhar tal desenvolvimento acarreta numa maior necessidade e preparação da polícia investigativa para a colheita de elementos probatório. Deste modo. o aprimoramento e capacitação dos agentes com fito de seguir o progresso tecnológico, atrelado à criação de leis específicas que colaborem à instrução processual tornam-se imprescindíveis ao exercício da pretensão punitiva (DORIGON; SOARES, 2017).

Nesse sentido, demonstra-se essencial a existência de uma polícia especificada em crimes cibernéticos, capacitadas e treinadas no campo tecnológico

e nas inovações perseverantes, de modo a criar uma verdadeira força tarefa à obtenção de todas as provas necessárias à obtenção do resultado desejado – instrução do processo penal (ALBUQUERQUE, 2006).

Daí também surge a necessidade de atuações preventivas, que, em tese, se dão por mecanismos tecnológicos, que melhor devem ser desenvolvidos e elucidados, tanto pelo provedor do serviço eletrônico, quanto pelas autoridades competentes ante a quaisquer falhas que tornem a segurança dos meios inapropriados para uso, sendo eles:

> “o controle de acesso subdividido em autorização e autenticação; dispositivos de defesa composto por um sistema ou um corpo de sistemas, que reforça o cumprimento de políticas de controle de acesso; "Virtual Private Network", que permite a troca de informações seguras por meio da utilização de redes públicas; monitoramento de arquivos de registros gerados pelos serviços de rede; sistemas compostos de hardware e software capazes de capturar informações; e a Criptografia e assinatura digital. (DOMINGUES; FINKELTEIN, 2003).

O problema do crime cibernético em si gira em torno do seu formato complexo, pela utilização de diversos meios e mecanismos, a volatilidade do fato em si ante a possibilidade de serem os dados apagados, alterados ou até perdidos, bem como a infinitude dos dados utilizados que necessitam de uma eficaz perícia em tempo hábil frente ao perigo de perecimento das provas (BRAGA, 2018).

Ante a desnecessidade física da presença do autor ao acometimento do ilícito, torna-se a imputação objetiva do fato extremamente complexo, isto porque são pouquíssimos os dados coletados e capazes de ensejar a autoria delitiva do agente. Um importante meio de conhecimento do possível autor do crime cibernético se dá por meio do reconhecimento do número IP atrelado ao computador, smartphone quaisquer outros aparelhos que possuem comunicação a internet. Tal número é uma espécie de código de registro do meio utilizado, de maneira que serve como uma identidade a qualquer ato realizado no meio eletrônico, uma espécie de digital eletrônica. Entretanto, o IP dá instrução ao investigador ao aparelho utilizado, mas não dá exatidão ao agente que utilizou, devendo ser utilizado como meio de obtenção da autoria delitiva (BRAGA, 2018; DORIGON; SOARES, 2017).

Em tese, ao acessar a rede de internet, é designada ao usuário um úmero de IP, entretanto tal número só lhe é atribuído no momento da conexão ao provedor de internet de modo que ao desliga-lo o número de IP será redesignado à outra pessoa, se não for optado pela parte por um IP estável. Assim, há uma possibilidade de

alteração constante do IP utilizado pelo usuário, de modo que sempre está em constância a utilização de um número específico, devendo ser localizado e compreendido o momento que o infrator utilizou-se do meio para avaliar a autoria delitiva. (BRAGA, 2018; SANTOS *et al*, 2014)

Daí surge um outro importante ponto: os servidores proxies, servidores que funcionam na intermediação das requisições dos usuários junto à rede, isto é, conectam uma vontade do agente à um serviço ou recurso disponível na rede. Nesse interim, ao valer-se de qualquer serviço ou requisição na rede constará o endereço IP do servidor proxy de quem teve acesso ao conteúdo disposto na internet, havendo uma espécie de omissão do IP do agente, aparecendo o IP do servidor proxy (DORIGON; SOARES, 2017).

Isto ocorre porque, inicialmente, o intuito dos servidores proxy era de omitir o endereço IP com vistas a proteger o usuário de possíveis crimes na rede, entretanto, a banalização de seu uso por agentes mal-intencionados ocasionou a eles uma ferramenta/meio para o acometimento de crimes: possível anonimato. São então denominados proxys anônimos que retiram quaisquer vestígios do ato praticado, uma vez que são suprimidos os dados necessários ao reconhecimento do autor e da identificação do comutador utilizado para tal (DORIGON; SOARES, 2017).

Aqueles que conhecem da rede e seus artifícios sabem como burlar tanto o endereço IP quanto os servidores consegue facilmente mudar sua identidade, seu endereço IP e até mesmo atribuir a outrem a autoria de seus atos por meio de alterações no próprio sistema informático. Desta maneira, os ditos hackers possuem um enorme controle na realização e ocultação de crimes cibernéticos, uma vez que conhecem os artifícios necessários à realização do ato (FUCHS; STUANI, 2021)

Em matéria constitucional, há provas que somente podem ser realizadas mediante perícia técnica após autorização judicial para verificar o IP da máquina utilizada, os servidores proxy e dados armazenados pelo usuário, que, se não realizados em conformidade com as determinações legais, serão desentranhadas do processo e consideradas ilícitas; doutro lado mora o perigo da obtenção da ordem judicial que demore a ser expedida, podendo comprometer a eficácia da medida que se visa.

Outro ponto importante se dá pela constatação da competência par o julgamento do fato delituoso, isto se dá porque temos crimes plurilocais, ou à distância, que dizer, há a desnecessidade da presença física do agente para o

acometimento do crime. Daí surge a imprescindibilidade da manutenção da legislação vigente à implementar o trabalho da polícia investigativa, uma vez que os dados de Proxy e IP são fornecidos pela operadoras de internet, e, muito das vezes a ausência do resultado das requisições tornam o serviço extremamente dificultoso.

Quer dizer, há uma maior necessidade de comunicação da vítima, da atividade investigativa e das operadoras de serviço, bem como de uma rede de compartilhamento de informações acerca das apurações em progresso, de modo que o compartilhamento de informações se torne a regra. O problema é que há uma espécie de escassez de profissionais qualificados para instrução da atividade investigativa e, pela dificuldade de obtenção de elementos probatórios por um agente não especializado na área é quase nulo, sendo somente mais um contratempo à elucidação do fato, daí uma rede de gerenciamento e compartilhamento de elementos colhidos auxilia diversos casos (SILVA; SILVA, 2019).

A investigação policial, nessas hipóteses, necessita de um profissional competente e qualificado, apto a realizar e emitir laudo pericial indicando todo o caminho que fora realizado para instruir os elementos de materialidade e autoria aptos a ensejar a perfeita individualização do agente. Isto, porque diante à complexidade dos dados tecnológicos e seu incrível avanço temporal, surge a necessidade da polícia investigativa acompanha-lo como forma a reduzir os empecilhos do atraso informacional. Noutro prisma, surge, ainda, a necessidade de uma legislação específica tipificando, de maneira ímpar, as condutas próprias como crimes cibernéticos, uma vez que fogem à simples constatação por outros tipos, valendo-se da especificidade de condutas (MEDEIROS; UGALDE, 2020).

5. CONCLUSÃO

Diante da pesquisa realizada, tornou-se possível compreender tanto a legislação vigente e antiga, quanto o crime cibernético, as espécies de crime mais comuns, e seu aumento diante da pandemia do COVID-19, sendo ao final aferido a atividade investigativa e seus dilemas contemporâneoa dado ao avanço tecnológico.

Em suma, pode-se dizer que com a crescente popularidade dos meios digitais, os crimes cibernéticos também tem aumentando, ainda mais em períodos de isolamento social. A facilidade do anonimato e a utilização de meios idôneos ao

cometimento do crime pelo meio virtuam contribuem de maneira signiticativa na prática de novos ilícitos.Verificou-se a problemática contida no presente trrabalho ao se evidenciar a complexidade existente nos crimes cibernéticos, tanto as modalidades criminosas quanto à necessária intervenção da polícia investigativa a promover diligências com fito de colecionar elementos de prova aptos a contribuir no exercício da demanda punitiva estatal.

Destarte, as dificuldades encontradas pela polícia e pelo judiciário em localizar os criminosos para efetivação da aplicação de sanções substantivas e imponentes têm contribuído para a impunidade e o crescente crime digital desenfreado. Nesse ponto, dado o avanço tecnológico, torna-se imprescindível que o Estado o acompanhe, de maneira que qualifique a atividade policial, instrua a condução criminal do fato para ao final aplicar a reprimenta ao ato criminoso.

Conclui-se, portanto, que o combate ao crime digital é uma questão complexa, que envolve a necessidade de formularem leis de combate aos crimes digitais, investir na estrutura e preparação da polícia investigativa para identificar e reprimir os criminosos e formular políticas públicas para orientar o geral público acerca dos possíveis delitos aplicados buscando a prevenção.

REFERÊNCIAS BIBLIOGRÁFICAS

AKCHAR, Jamili. **Breve análise dos princípios essenciais do Marco Civil da Internet**. Disponível em: <https://jamili.jusbrasil.com.br/artigos/435150451/breve-analise-dos-principiosessenciais-do-marco-civil-da-internet-lei-129654#:~:text=O%2520Marco%2520Civil%2520da%2520Internet,da%2520rede%252C%2520conforme%252 0a%2520seguir>. Acesso em: 27 set. 2021.

ALBUQUERQUE, Roberto Chacon de. **A criminalidade informática**. São Paulo: Editora Juarez de Oliveita, 2006.

BRAGA, Diego Campos Salgado. **Métodos de investigação no âmbito cibernético**. Disponível em: <https://jus.com.br/artigos/71463/metodos-de-investigacoes-no-ambito-cibernetico>. Acesso em: 24 out. 2021.

CAPEZ, Fernando. **Curso de processo penal**. São Paulo: Saraiva, 2021.

CARNEIRO, Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação.** Disponível em: <https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-umareflexao-sobre-o-problema-natipificacao/#:~:text=Na década de 70 a,à necessi dade de se despender>. Acesso em: 20 set. 2021.

COUTINHO, Thiago de Miranda. **Crimes virtuais na pandemia: da prevenção à consumação do delito**. Disponível em: <https://canalcienciascriminais.com.br/crimes-virtuais-na-pandemia-da-prevencao-a-consumacao-do-delito/>. Acesso em: 25 out. 2021.

CORREIO BRASILIENSE. Com 17.843 ocorrências, crimes cometidos pela internet sobem 87,1% em 2020. 2021. Disponível em: <https://www.correiobraziliense.com.br/cidades-df/2021/02/4906387-com-17-843-ocorrencias-crimes-cometidos-pela-internet-sobem-871--em-2020.html>. Acesso em 13 set. 2021.

DORIGON, Alessandro; SOARES, Renan Vinicíus de Oliveira Soares. **Crimes cibernéticos: dificuldades para obter indícios de autoria e materialidade**. Disponível em: <https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade/4>. Acesso em: 24 out. 2021.

FUCHS, Pedro Henrique Camargo; STUANI, Willian Ricieri Dias. Crimes cibernéticos e a legislação brasileira. **Anuário Pesquisa e Extensão Unoesc São Miguel do Oeste**, 2021.

LEMOS, Ronaldo; LEITE, George Salomaão. **Marco civil da internet**. São Paulo: Atlas, 2014.

MARRA, Fabiane Barbosa. Desafios do Direito na Era da Internet: uma breve análise sobre os crimes cibernéticos. **CAMPO JURÍDICO**, v. 7, n. 2, p. 145–167, 12 dez. 2019. Disponível em: <http://fasb.edu.br/revista/index.php/campojuridico/article/view/289>. Acesso em: 24 out. 2021.

MARTINS, Humberto. **Seminário virtual: Criminalidade em tempo de Covid. Atuação do Sistema de Justiça.**

MEDEIROS, Gutembergue Silva; UGALDE, Júlio César Rodrigues. **Crimes Cibernéticos: Considerações Sobre a Criminalidade na Internet**. Disponível em: <MEDEIROS, Gutembergue Silva; UGALDE, Júlio César Rodrigues>. Acesso em: 24 set. 2020.

PEREIRA, Tacieli; PITON, Vinícius; ALBRECHT, Evandro Carlos. Qual a influência da pandemia do COVID-19 aos crimes cibernéticos? **Anuário Pesquisa e Extensão Unoesc São Miguel do Oeste**, v. 6, 2021.

SANTOS, Ederson Luiz Reis Dos. **Fenômenos criminológicos decorrentes da pandemia covid-19.** Disponível em: <https://jus.com.br/artigos/84677/fenomenos-criminologicos-decorrentes-dapandemia-covid-19>. Acesso em: 24 out. 2021.

SANTOS, Liara Ruff dos; MARTINS, Luana Bertasso; TYBUCSH, Francielle Benini Agne. Os crimes cibernéticos e o direito a segurança jurídica: uma análise da legislação vigente no cenário brasileiro contemporâneo. 2014. Disponível em: <http://coral.ufsm.br/congressodireito/anais/2017/7-7.pdf>. Acesso em: 18 ago.

2021.

SCHAUN, Guilherme. **Uma lista com 24 crimes virtuais**. Disponível em: <https://guilhermebsschaun.jusbrasil.com.br/artigos/686948017/uma-lista-com-24-crimes-virtuais.>. Acesso em: 9 set. 2021.

SERPRO. **O que muda com a LGPD**. Disponível em: <https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd>. Acesso em: 25 out. 2021.

SILVA, Kaique Rodrigues da; SILVA, Rubens Alves da. Crimes cibernéticos: necessidade de novas ferramentas de investigação com encargos no ônus da prova. **Revista Artigos. Com**, v. 12, 2019.