CENTRO UNIVERSITÁRIO DE GOIÁS – UNIGOIÁS
PRÓ-REITORIA DE ENSINO PRESENCIAL – PROEP
SUPERVISÃO DA ÁREA DE PESQUISA CIENTÍFICA – SAPC
CURSO DE DIREITO

A EVOLUÇÃO E AS DIFICULDADES NA COLHEITA DE ELEMENTOS DE AUTORIA DELITIVA DOS CRIMES CIBERNÉTICOS

BRUNO HENRIQUE TEIXEIRA DOS SANTOS
ORIENTADORA: CASSIRA LOURDES DE ALCÂNTARA DIAS RAMOS JUBÉ

GOIÂNIA
JUNHO/2022

BRUNO HENRIQUE TEIXEIRA DOS SANTOS

A EVOLUÇÃO E AS DIFICULDADES NA COLHEITA DE ELEMENTOS DE AUTORIA DELITIVA DOS CRIMES CIBERNÉTICOS

Trabalho final de curso apresentado e julgado como requisito para a obtenção do grau de bacharelado no curso de Direito do Centro Universitário de Goiás – UNIGOIÁS na data de 07 de junho de 2022.

Profa. Mestre Cassira Lourdes de Alcântara Dias Ramos Jubé (Orientadora)
Centro Universitário de Goiás – UNIGOIÁS

Prof. Mestre José Cristiano Leão Tolini (Examinador)
Centro Universitário de Goiás – UNIGOIÁS

A EVOLUÇÃO E AS DIFICULDADES NA COLHEITA DE ELEMENTOS DE AUTORIA DELITIVA DOS CRIMES CIBERNÉTICOS

Bruno Henrique Teixeira dos Santos[1]
Orientadora: Cassira Lourdes de Alcântara Dias Ramos Jubé[2]

Resumo: A presente pesquisa, tem o intuito de abordar a teoria dos crimes em geral tendo como foco os crimes virtuais. Foi utilizado a metodologia bibliográfica, utilizando livros, artigos sobre o tema e análises de jornais de livre circulação publicados no país. A presente, faz uma análise sobre os crimes e suas espécies, detalhando assim as categorias mais relevantes no nosso ordenamento, também foi abordado as suas classificações, trazendo uma especificação bem ampla e clara sobre o assunto. Além do mais, foi abordado de forma geral os crimes cibernéticos, presente na lei 12.737/2012, trazendo suas ramificações na lei e as dificuldades encontradas para combater este tipo de crime. Analisando assim todas as formas necessárias para que seja investigado e julgado o crime, baseando-se nos mecanismos criados ao longo do tempo, explorando a dificuldade na obtenção de provas deste delito, e os problemas na identificação da autoria. Trazendo também toda evolução histórica deste crime, desde que foram criados até os dias atuais, conceituando-os assim para o melhor entendimento. Desta forma, o presente trabalho trouxe uma análise sobre a tipificação em geral dos crimes na lei, bem como expor as lacunas encontradas no ordenamento causando assim uma crise na coleta de provas e na identificação da autoria.

Palavras-chave: Crimes Virtuais. Tipificação. Coleta de Provas. Investigação.

THE EVOLUTION AND DIFFICULTIES IN COLLECTING ELEMENTS OF CRIMINAL AUTHORSHIP IN CYBERCRIME

Abstract: The present research aims to address the theory of crimes in general focusing on cybercrimes. The bibliographic methodology was used, using books, articles on the subject and analysis of newspapers of free circulation published in the country. The present study analyzes the crimes and their species, thus detailing the most relevant categories in our legal system; its classifications were also addressed, bringing a very broad and clear specification on the subject. Moreover, it was addressed in a general way the cybercrimes, present in law 12.737/2012, bringing their ramifications in law and the difficulties encountered to combat this type of crime. Analyzing all the necessary ways to investigate and prosecute the crime, based on the mechanisms created over time, exploring the difficulty in obtaining evidence of this crime, and the problems in identifying the authorship. It also brings all the historical evolution of this crime, since they were created until the present days, thus conceptualizing them for a better understanding. Thus, the present work brought an analysis of the general typification of crimes in the law, as well as exposing the gaps found in the legal system, thus causing a crisis in the collection of evidence and the identification of authorship.

Keywords: Virtual Crimes. Typification. Evidence Gathering. Investigation.

[1] Discente do Curso de Direito do Centro Universitário de Goiás – UNIGOIÁS. Lattes: http://lattes.cnpq.br/2006301421324286. E-mail: 19onurb@gmail.com
[2] Professora Adjunta do Centro Universitário de Goiás – UNIGOIÁS. Graduada em Direito pela Pontifícia Universidade Católica de Goiás; advogada; Especialista em Direitos Humanos pela Academia de Polícia Militar e Docência Universitária pela Universidade Estadual de Goiás; e Mestre em Direitos Humanos pela Universidade Federal de Goiás; Lattes: http://lattes.cnpq.br/6792979547523586 E-mail: cassiralourdes@gmail.com

INTRODUÇÃO

Os crimes cibernéticos fazem parte da nossa sociedade a muito tempo, desde a popularização da internet e das redes sociais esse crime tem causado problemas entre as pessoas. Sendo assim, essa atitude de praticar crimes virtualmente tem se tornado popular pela facilidade de se esconder atrás de uma tela sem ser encontrado facilmente.

Dessa forma, o presente instrumento tem como objetivo fazer um estudo detalhado sobre os mecanismos criados ao longo do tempo, cuja finalidade é combater esse tipo de crime, sanando todas as dificuldades encontradas na obtenção de provas contra o autor.

A pesquisa irá trazer em sua integridade as leis esparsas, que tem por objetivo encontrar todas as dificuldades que existem para encontrar os autores deste crime, assim como erradicar essa conduta, como por exemplo a Lei n.º 12.737 de 2012, que tem como finalidade tipificar e informar sobre os delitos informáticos.

Desse modo, a atuação criminosa é um fator preocupante, principalmente no que tange o cumprimento das leis, visto que a identificação dos criminosos é, na maioria das vezes, difícil de ser realizada, mantendo-os acobertados pelo anonimato e consequentemente, impunes.

Diante disso, levanta-se a seguinte problematização, devido os autores dos crimes cibernéticos compreenderem a dificuldade de sua identificação, a ocorrência dos crimes cresce de forma considerável, tornando-se um fator a ser debatido judicialmente.

Machado (2017, p. 7), cita "a falta de norma incriminadora para algumas condutas praticadas por meio dos sistemas informáticos, dificultam a aplicação de uma sanção adequada para os que praticam condutas ilícitas […]".

Olavo Filho (2017), destaca que atualmente no Brasil temos poucas leis que punem os crimes praticados através da internet, onde o legislador teve boa vontade em buscar uma maneira de combater a problemática tratada, porém falhou em penalizar de maneira correta.

E para o levantamento das referências, pesquisou-se pelas seguintes palavras chaves: Crimes cibernéticos, Evolução tecnológica; Evolução dos crimes virtuais; Espécie dos crimes; Legislação. Segundo Gil (2002), permitem o levantamento dos dados utilizando como seleção, referências adequadas ao tema tratado e de autores conhecidos, facilitando a elaboração do trabalho.

METODOLOGIA

O presente projeto de pesquisa faz uma abordagem qualiquantitativa, vez que o mesmo possui embasamento em informações, posicionamentos doutrinários, artigos acadêmicos, legislações, informações de livros, e principalmente em dados colhidos na lei.

Ademais, trata-se de uma pesquisa exploratória, visto que o objetivo principal é analisar detalhadamente as inovações introduzidas pela Lei n.º 12.737, de 30 de novembro de 2012, tipificando os delitos informáticos e determinando o posicionamento contra este crime.

Diante disso, em relação as técnicas de pesquisa o referido projeto utiliza-se da revisão bibliográfica, visando abordar um grande leque de informações. Sendo assim, são feitos posicionamentos com base em conceitos doutrinários, mostrando o "mundo" jurídico de acordo com o pensamento de estudiosos, também se utiliza de legislações para analisar as mudanças em relação as leis ao longo do tempo e por fim o uso de convenções e artigos científicos.

1 TEORIA GERAL DOS CRIMES

Todo crime vem de uma ação humana, até que se prove o contrário, apenas os seres humanos são imputáveis, ou seja, passíveis de serem responsabilizados por seus próprios atos. Existem pessoas que não tem essa capacidade, obviamente, seja pela idade ou pelo desenvolvimento mental, recebendo assim sanções diferenciadas (PASCHOAL, 2015).

Primeiramente, é preciso diferenciar crime de contravenção penal. Ambos são infrações penais, todavia, contravenção é regulada pelo Decreto-lei n.º 3.688, de 3 de outubro de 1941, enquanto os atos considerados como crimes estão tipificados, em grande parte, no Código Penal Brasileiro (BRASIL, 1940). A principal diferença entre os dois é em relação a pena, para os crimes a lei prevê prisão de reclusão ou detenção, que pode chegar até a 30 anos, já na contravenção a lei prevê pena de prisão simples, que na prática se assemelha a detenção, podendo chegar no máximo a 5 anos.

Quando é falado do conceito de crime, no Brasil não temos um termo certo, é um conceito ainda vago, que irá se aperfeiçoando ao longo dos anos.

> Embora a Lei de Introdução ao Código Penal nos forneça um critério de distinção entre o crime e a contravenção penal, pela leitura do seu art. 1º não conseguimos destacar os elementos ou características indispensáveis ao conceito de infração penal. Esse, na verdade, é um conceito que veio evoluindo ao longo dos anos, sendo que várias teorias surgiram com a finalidade de explicá-lo. (GRECO, 2020, p. 27)

Para se estudar crime, devemos nos atentar aos seus sistemas, sendo eles formal; material; formal e material; formal, material e sintomático. Formalmente conceitua-se sob o aspecto da técnica jurídica, tendo em vista a lei. Materialmente, tem-se o crime sob o ângulo ontológico, objetivando a razão em que o legislador determinou a conduta como criminosa, a sua natureza danosa e suas consequências.

O conceito material de crime é de relevância jurídica, tendo em vista o seu destaque no conteúdo teleológico, determinando a razão de constituir uma conduta humana à infração penal sujeita a uma sanção. Sem uma descrição legal, é certo de que nenhum fato pode ser considerado crime, todavia, é necessário estabelecer critérios para que o legislador determine um ato como criminoso. É preciso que o legislador tenha um norte, pois, de forma contrária, ficaria ao seu critério a criação das normas penais, lesando o direito à liberdade dos cidadãos.

Para Jiménez de Asúa (1951 *apud* MIRABETE; FABBRINI, 2007, p. 82), "crime é a conduta considerada pelo legislador como contrária a uma norma de cultura reconhecida pelo Estado e lesiva de bens juridicamente protegidos, procedente de um homem imputável que manifesta com sua agressão perigosidade social".

No sentido substancial, delito é a ação ou omissão, imputável a uma pessoa, sendo lesiva ou perigosa a algum interesse penalmente protegido, constituída a determinados elementos e integrada a certas condições, ou acompanhadas de certas circunstâncias previstas em lei (BITENCOURT, 2020).

Assim, verifica-se que para que se tenha um crime, é necessário que haja um comportamento de caráter lesivo, sendo capaz de resultar em um dano social que afete a condição de existência, conservação e desenvolvimento da sociedade.

> Pode-se concluir que, para o legislador definir certo fato humano como crime, deve, previamente, verificar se o mesmo é daqueles que lesionam bens jurídicos, ou pelo menos expõem-nos a grave perigo de lesão, e se tais lesões são de gravidade acentuada, de modo a serem proibidas sob ameaça da pena criminal. Do contrário, não poderá o legislador considerá-las crime. (TELES, 2004, p. 153)

Como foi observado, sob o ponto de vista material, o conceito de crime visa os bens protegidos pela lei penal, dessa forma, nada mais é do que a violação de um bem penalmente protegido.

O conceito formal de crime, nada mais é que o fato estabelecido em lei como proibido e ao qual se comina uma sanção penal. Para Teles (2004, p. 152), "o crime do ponto de vista formal, é o comportamento humano, proibido pela norma penal, ou, simplesmente, a violação desta norma".

Crime é, portanto, aquela conduta vedada pela legislação penal.

> Segundo a concepção formal, crime é a conduta proibida e sancionada pela lei penal. É exatamente esse caráter de pura contrariedade formal ao Direito, que é acentuado nessa definição: crime é toda ação ou omissão proibida pela lei, sob ameaça de pena. É como se a nocividade, a perversidade, a imoralidade ou o caráter antissocial da

> conduta ilícita surgisse com a promulgação da norma incriminadora ou fosse pura criação desta. (LEAL, 2004, p. 181)

Sob aspecto formal, crime é um fato típico e antijurídico.

> Fato típico é o comportamento humano (positivo ou negativo) que provoca um resultado (em regra) e é previsto na lei penal como infração. Assim, fato típico do homicídio é a conduta humana que causa a morte de um homem. Ex.: A esfaqueia B, que vem a morrer em consequência das lesões. O fato se enquadra na descrição legal simples do art. 121 do CP: 'Matar alguém'. (JESUS; ESTEFAM, 2020, p. 187)

Outro componente e não menos importante que faz parte da teoria geral do crime, e que pode ser conceituado sob o aspecto formal, trata-se da antijuridicidade. Essa característica como elemento para a tipificação do crime, aborda no artigo 23, do Código Penal Brasileiro, as formas em que o agente não deve estar, ou seja, trata-se de excludentes de ilicitude, excluindo o crime caso o agente se encontre em alguma das situações *in verbis*:

> Art. 23 - Não há crime quando o agente pratica o fato: (Redação dada pela Lei nº 7.209, de 11.7.1984)
> I - Em estado de necessidade; (Incluído pela Lei nº 7.209, de 11.7.1984)
> II - Em legítima defesa; (Incluído pela Lei nº 7.209, de 11.7.1984) (Vide ADPF 779)
> III - Em estrito cumprimento de dever legal ou no exercício regular de direito. (Incluído pela Lei nº 7.209, de 11.7.1984). (BRASIL, 1940, n. p.)

No entanto, é importante ressaltar a diferença entre essas excludentes, sendo necessário abordar cada uma de forma individual.

O estado de necessidade, é uma situação especial em que há o sacrifício de um direito juridicamente protegido, para salvar de perigo atual e inevitável o direito do próprio agente ou de um terceiro, como é dito no artigo 24 do Código Penal Brasileiro:

> Art. 24 - Considera-se em estado de necessidade quem pratica o fato para salvar de perigo atual, que não provocou por sua vontade, nem podia de outro modo evitar, direito próprio ou alheio, cujo sacrifício, nas circunstâncias, não era razoável exigir-se:
> § 1º - Não pode alegar estado de necessidade quem tinha o dever legal de enfrentar o perigo.
> § 2º - Embora seja razoável exigir-se o sacrifício do direito ameaçado, a pena poderá ser reduzida de um a dois terços. (BRASIL, 1940, n. p.)

A legítima defesa, trata-se de uma forma de repelir uma injusta agressão atual ou iminente, sendo possível a responsabilização pelo excesso, como é dito no artigo 25 do Código Penal Brasileiro:

> Art. 25 - Entende-se em legítima defesa quem, usando moderadamente dos meios necessários, repele injusta agressão, atual ou iminente, a direito seu ou de outrem.
> Parágrafo único. Observados os requisitos previstos no caput deste artigo, considera-se também em legítima defesa o agente de segurança pública que repele agressão ou risco de agressão a vítima mantida refém durante a prática de crimes. (BRASIL, 1940, n. p.)

O Código não cuidou de conceituar essa excludente diretamente, porém seu conceito pode ser extraído da sua própria expressão, sendo assim, o estrito cumprimento do dever legal é uma causa que ocorre em casos de funcionários públicos, ou agentes que exerçam a função, os quais em que determinadas situações são obrigados a violar o bem jurídico de indivíduos para estabelecer um dever legal.

1.1 CLASSIFICAÇÃO DOS CRIMES

Os crimes são divididos em alguns tópicos, para que seja mais fácil a sua compreensão e seu estudo, sendo eles os crimes comuns, próprios, instantâneos, permanentes, comissivos, omissivos, crimes de atividade, de resultado, de dano, de perigo, crimes unissubjetivos e plurissubjetivos, progressivos, complexos, entre outros.

Os crimes comuns são aqueles que podem ser praticados por qualquer pessoa, como por exemplo o homicídio ou o roubo. Em contrapartida os crimes próprios são os que exigem um sujeito ativo especial, podendo ser praticados somente por pessoas com determinadas qualidades. Tais qualidades podem se referir tanto a natureza humana, como o exemplo da mãe praticando o infanticídio, quanto a lei, como a testemunha no crime de falso testemunho (NUCCI, 2022).

> Os próprios podem ser subdivididos em puros e impuros. Os primeiros dizem respeito aos delitos que, quando não forem cometidos pelo sujeito indicado no tipo penal, deixam de ser crimes, caso a conduta se concretize por ato de outra pessoa (ex.: advocacia administrativa – art. 321. Nesse caso, somente o funcionário pode praticar a conduta; outra pessoa que o faça não prática infração penal). Os impuros referem-se aos delitos que, se não cometidos pelo agente indicado no tipo penal, transformam-se em figuras delituosas diversas (ex.: se a mãe mata o filho recém-nascido, após o parto, em estado puerperal, é infanticídio; caso um estranho mate o recém-nascido, sem qualquer participação da mãe, cuida-se de homicídio). (NUCCI, 2022, p. 117)

Os crimes instantâneos são aqueles que se consumam com uma única conduta e não irão produzir resultado ao longo do tempo, embora a ação possa perdurar, como o homicídio, o roubo. Já os delitos permanentes são os que se consumam com uma única conduta, porém a situação irá perdurar durante o tempo em que o agente tiver vontade, como o sequestro, em que a vítima terá sua liberdade tirada, e permanecerá em cativeiro pelo tempo que o agente quiser.

> Os delitos instantâneos são aqueles cuja consumação se dá com uma única conduta e não produzem um resultado prolongado no tempo. Assim, ainda que a ação possa ser arrastada no tempo, o resultado é sempre instantâneo (ex.: homicídio, furto, roubo).
> Os delitos permanentes são os que se consumam com uma única conduta, embora a situação antijurídica gerada se prolongue no tempo até quando queira o agente. Exemplo disso é o sequestro ou cárcere privado. Com a ação de tirar a liberdade da vítima, o delito está consumado, embora, enquanto esteja está em cativeiro, por vontade do agente, continue o delito em franca realização. Outros exemplos: extorsão mediante sequestro, porte ilegal de arma e de substância entorpecente. (NUCCI, 2022, p. 118)

São crimes comissivos aqueles praticados por um comportamento positivo do agente, isto é, um fazer como o estupro e o furto. Já os omissivos são aqueles praticados por um comportamento negativo, uma abstenção, um não fazer, como a omissão de socorro. Os crimes omissivos são divididos em próprios, que são aqueles previstos em um tipo mandamental, tornando criminosa a abstenção em determinadas circunstâncias, e impróprios, em que o sujeito tem o dever de evitar o resultado naturalístico, que é dito no artigo 13, parágrafo segundo:

> Art. 13 - O resultado, de que depende a existência do crime, somente é imputável a quem lhe deu causa. Considera-se causa a ação ou omissão sem a qual o resultado não teria ocorrido. […]
> § 2º - A omissão é penalmente relevante quando o omitente devia e podia agir para evitar o resultado. O dever de agir incumbe a quem:
> a) tenha por lei obrigação de cuidado, proteção ou vigilância;
> b) de outra forma, assumiu a responsabilidade de impedir o resultado;
> c) com seu comportamento anterior, criou o risco da ocorrência do resultado. (BRASIL, 1940, n. p.)

Os crimes de atividade são aqueles que não exigem um certo resultado naturalístico para sua consumação e contentam-se com a mera ação humana, sendo suficiente para se esgotar o tipo penal, chamados também de crimes formais ou de mera conduta, como a prevaricação que mesmo não havendo efeitos no mundo naturalístico o agente é punido.

> Chamam-se delitos de atividade os que se contentam com a ação humana esgotando a descrição típica, havendo ou não resultado naturalístico. São chamados de formais ou de mera conduta. Exemplo: prevaricação (art. 319). Contenta-se o tipo penal em prever punição para o agente que deixar de praticar ato de ofício para satisfazer interesse pessoal, ainda que, efetivamente, nada ocorra no mundo naturalístico, ou seja, mesmo que nenhum prejuízo efetivo se materialize. (NUCCI, 2022, p. 119)

Já os crimes de resultado são os que dependem de um resultado naturalístico, sem este não existe a consumação, e sim a tentativa.

> Por outro lado, denominam-se crimes de resultado (também chamados de materiais ou causais) aqueles que necessariamente possuem resultado naturalístico; sem a sua ocorrência, o delito é apenas uma tentativa. Ex.: furto. Se a coisa for retirada da esfera de proteção e vigilância do proprietário, consuma-se o delito. Do contrário, caso o resultado naturalístico não se dê por circunstâncias alheias à vontade do agente, temos apenas uma tentativa de furto. (NUCCI, 2022, p. 119)

O crime habitual se consuma apenas através da prática reiterada e contínua de várias condutas consideradas atípicas, fazendo com que seja punido o conjunto de ações praticadas. Tendo assim três requisitos, a reiteração de vários fatos, a identidade dos fatos e o nexo de habitualidade entre os fatos.

> É modalidade específica de crime, não admitindo confusão com os instantâneos e os permanentes. Configura-se, em nosso entender, equívoco a classificação que aponta a convivência da habitualidade com a permanência, isto é, o crime habitual não é permanente e vice-versa. O delito permanente consuma-se numa única conduta e o resultado prolonga-se no tempo, enquanto o habitual exige a prática de várias condutas, analisadas em conjunto no momento da aplicação da lei penal, a fim de se verificar se houve ou não habitualidade. Logo, os crimes habituais, diferentemente dos permanentes, não admitem tentativa, nem tampouco suportam prisão em flagrante. (NUCCI, 2022, p. 122)

Há também uma distinção entre crime habitual próprio e crime habitual impróprio, dizendo assim Nucci (2022, p. 150):

> Deve-se, ainda, distinguir o crime habitual próprio do habitual impróprio. Próprio é o delito habitual autêntico (cuida-se da denominada habitualidade constitutiva), que somente se tipifica apurando-se a reiteração de condutas do agente, de modo a configurar um estilo próprio de vida, enquanto o impróprio (a chamada habitualidade delitiva) é a reiteração na prática de crimes instantâneos ou permanentes (ex.: pessoa que vive do cometimento de furtos repetidamente realizados).

Existem outras várias classificações de crimes na nossa lei, como o de perigo, unissubjetivos e plurissubjetivos, progressivos, complexos, dentre outros não menos importantes.

2 ASPECTOS HISTÓRICOS E CONCEITUAIS DOS CRIMES CIBERNÉTICOS

A internet, também conhecida como “rede mundial de computadores”, surgiu durante a guerra fria, com a única e exclusiva finalidade de proteger os computadores e informações do Governo Norte Americano. Além do mais, em determinado tempo, a utilização da internet era restrita as áreas militares e universitárias, somente no início da década de 1980 que o sistema passou a ser utilizado para o comércio. No Brasil, o Ministério da Ciência e Tecnologia do Brasil, define a Internet como um sistema de rede de computadores – uma rede de redes – que

pode ser utilizado por qualquer pessoa em qualquer parte do mundo, onde haja um ponto de acesso.

Notavelmente a internet apresenta inúmeras vantagens e benefícios para as pessoas, vez que reduziu as distâncias entre elas, possibilitando a realização de relações sociais e comerciais entre pessoas que antes era quase impossível, fato que possibilitou um imenso crescimento econômico nos países que estão conectados à internet.

Percebe-se que a utilização da internet está relacionada a várias atividades do nosso cotidiano, o que nos faz reconhecer que a mesma está modificando as nossas relações sociais, pessoais, profissionais e financeiras, sendo que, de igual forma está criando diversas condutas danosas a nossa sociedade, ou seja, a conduta criminosa está se aperfeiçoando na mesma proporção do desenvolvimento da internet.

O ciberespaço é um espaço virtual abrangido pela internet que reduziu fronteiras e aproximaram as pessoas, formando uma nova dimensão espacial que permite todos aqueles conectados à rede um contato imediato com qualquer pessoa no mundo em segundos. Deste modo, pode – se perceber que da mesma forma que a internet traz benefícios imensuráveis a população, também proporciona práticas ilícitas que podem causar danos as pessoas conectadas.

> Poderíamos dizer que os ‘crimes’ digitais seriam todos aqueles relacionados ‘as informações arquivadas ou em trânsito por computadores’, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar; para tal prática é indispensável a utilização de um meio eletrônico. Toda sociedade dependente da informação acaba sendo vítima de simples ameaças e até do terrorismo e do vandalismo eletrônicos. (CORRÊA, 2010, p. 43)

Tais crimes, podem ser divididos em vários tipos diferentes, como a pornografia, que em si só já se divide em 3 categorias, a relacionada a publicação sem haver constrangimentos, a das publicações online onde se cobra para a visualização e a última que é relacionada a pedofilia e a materiais obscenos.

> A ‘pirataria’ de software consiste na apropriação e venda de cópias de programas de computador sem a licença do autor, estando regulada no Brasil pela Lei n. 9.609, de 19 de fevereiro de 1998, que dispõe sobre a proteção da propriedade intelectual de programa de computador e sua comercialização no País. (CORRÊA, 2010, p. 46-47)

A cópia ilegal no Brasil tem penas que podem ser de detenção de 6 meses a 2 anos, ou até mesmo 4 anos de reclusão, contendo também a possibilidade de uma condenação ao pagamento de indenizações milionárias.

> A lavagem está baseada em uma cadeia de rápidas transações, envolvendo mais do que a mera movimentação de dinheiro dentro do país; envolve também a movimentação para fora do país, para fora do controle jurisdicional, tornando o seu rastreamento e controle quase impossível. (CORRÊA, 2010, p. 54)

Levando em consideração os fatos, esse dinheiro deveria ser tributado e confiscado, porém os criminosos fazem o uso de bancos que realizam transações em formatos criptografados internacionalmente, sendo impossível ser reconhecido por terceiros, fazendo com que não sejam computados na receita.

> Poderíamos dizer que o hacker é um indivíduo que tem a intenção, através do computador, de adentrar um sistema sem ter autorização. Hacking seria esse ato. Seria o mesmo que ultrapassar, quebrar ou entrar em algum lugar para o qual é necessária prévia autorização. (CORRÊA, 2010, p. 57)

Os primeiros casos de crimes virtuais ocorreram na década de 1960, onde os infratores manipulavam os dados contidos nos computadores, praticando atos de sabotagem, espionagem e abuso ilegal de sistema, contudo, era muito difícil detectar a prática de tal ato devido as condições técnicas daquela época. Sendo assim, a partir de 1980 houve uma alteração sobre o tema, sendo identificadas e divulgadas várias ações criminosas, como pirataria de programas, manipulação de valores nos caixas eletrônicos etc. Assim, com essa intensa prática de delitos informáticos durante esse período, foram sendo criadas as primeiras legislações que regulamentavam a prática de tais atos ilícitos.

Os Estados Unidos da América foram os pioneiros no assunto, criando em 1984 a legislação “Crime Control Act” e logo depois “Computer Fraud and Abuse Act” em 1986. A Alemanha, também em 1986, criou a lei “Computer Kriminalitat”, seguida da França com a lei “Godfrain” em 1988. Posteriormente, em 1995, a Espanha incluiu no seu código penal os crimes de informática. Em 2001, o Conselho da Europa elaborou a Convenção Europeia Sobre Crimes Cibernéticos, também conhecida domo Convenção de Budapeste, tendo como o objetivo uniformizar a legislação europeia quanto a política criminal dos crimes cibernéticos.

A convenção foi dividida em quatro capítulos, tendo 5 títulos, o primeiro trata das terminologias, já nos outros capítulos estão previstas as medidas para serem tomadas no âmbito das legislações nacionais, criando leis penais, normas e criminalizando certas condutas. Podemos destacar, que a Convenção dispõe que quando existir pluralidade de partes reivindicando a competência para processar e julgar a prática de uma suposta infração prevista

na convenção, todas as partes envolvidas devem se reunir para consentir uma decisão mais apropriada.

Como foi dito, Convenção de Budapeste é um importante instrumento de combate aos crimes cibernéticos, pois além de unir os países signatários para regulamentar um problema em comum, procura uniformizar as normas de combate à prática destes crimes. O Brasil, por sua vez, ainda não é um país signatário da Convenção de Budapeste, contudo, já regulamentou algumas normas com a mesma finalidade, ou seja, de regulamentar o uso da internet pelos seus usuários e criminalizar condutas ilícitas praticadas via internet.

No Brasil, o tema foi inicialmente tratado como uma questão de direito penal econômico, sendo que em 1987 foi editada a Lei n.º 7.646, que tinha por finalidade a proteção à propriedade intelectual sobre programas de computador e sua comercialização no país. Sendo revogada depois pelo artigo 16 da Lei n.º 9.609/1998. Mais tarde, foi editada a Lei n.º 8.137/1990, que define crimes praticados contra a ordem tributária. Somente com a edição da Lei n.º 9.883/2000, que o legislador passou a abranger a regulamentação de outros delitos relacionados a internet que não eram de ordem econômica, tendo como finalidade proteger os dados e os sistemas de informação, punindo principalmente os crimes próprios de funcionários públicos que violem o sistema de informação da Administração Pública.

Recentemente, houve a edição da Lei n.º 12.695/2014, popularmente conhecida como "Marco Civil da Internet", que regulamenta a utilização da internet, estabelecendo princípios e normas que asseguram uma maior proteção aos usuários da internet. Tal lei foi criada através de uma junção de vários projetos parecidos, que ganharam força principalmente pelas descobertas de espionagem do Governo Norte Americano contra o Brasil e outros países.

O capítulo I dispõe sobre conceitos, princípios, direitos e deveres para a utilização da internet a nível nacional, bem como estipula diretrizes para a atuação do poder público em relação à matéria. No capítulo II, fala sobre direitos e garantias dos usuários, estabelecendo proteção à intimidade e a vida privada dos usuários, além de assegurá-los o direito de informações claras e precisas quanto às políticas de uso dos sites, provedores e redes sociais (BRASIL, 2014).

O capítulo III estabelece provisão de conexão e de aplicações de internet, onde define inúmeras normas. A neutralidade da rede é uma das diretrizes que foram estabelecidas neste capítulo, sendo de fundamental importância, pois institui ao responsável pela transmissão, comutação ou roteamento da obrigação de tratar de forma isonômica qualquer pacote de dados, sem distinção pela sua origem, destino, conteúdo, serviço, terminal ou aplicação. Por outro lado,

o capítulo IV, aborda diretrizes para a atuação dos entes públicos no desenvolvimento da internet no Brasil (BRASIL, 2014).

Terminando assim, com o capítulo V, que dispõe sobre disposições finais estabelecendo a liberdade de escolha do usuário na utilização de programas de computador, além de estimular a defesa dos seus interesses e direitos estabelecidos na presente Lei no âmbito administrativo e judicial (BRASIL, 2014).

As leis Brasileiras tiveram duas fontes principais, sendo elas a Lei Federal de Abuso Computacional ("Computer Misuse Act") e a Lei de Fraudes e Abusos Cometidos por Computadores ("Computer Fraud and Abuse Act"). "A lei mais importante relacionada aos 'crimes' digitais nos Estados Unidos foi promulgada em 1986 […]. Tal lei tipificou atividades divididas em várias categorias" (CORRÊA, 2010, p. 65).

A maioria dos crimes cibernéticos são praticados com a utilização de softwares criminosos, como os *cookies*; *spyware*; Cavalo de Troia; vírus etc. Destaca-se, tais crimes podem ser praticados por qualquer pessoa, porém, existem indivíduos específicos tais como os hackers. Ocorre que, a grande dificuldade é indicar com precisão o tempo e o local do crime. Isto porque, primeiro, no âmbito virtual não existem espaços físicos predeterminados, segundo, é possível programar a execução do crime no tempo. Desta forma, é essencial a identificação da localização da informação, pois será a partir desta constatação que proporcionará a ideia de território, para que, consequentemente, seja aplicada a sanção penal competente.

2.1 DA CLASSIFICAÇÃO

O que define o crime de informática é a utilização do computador ou da internet para a prática do ato, sendo classificados como crimes cibernéticos puros e impuros.

Os crimes cibernéticos puros, acontecem quando o agente quer atacar o sistema de informática de um terceiro, sendo ele um software, hardware ou um sistema de armazenamento de dados.

Segundo Damásio de Jesus e André Estefam (2020):

> Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado.

Podemos notar que esta categoria de crime é caracterizada quando um indivíduo, principalmente o hacker, utiliza-se de um computador e da internet em si para invadir a rede de

um terceiro, sendo o crime consumado no próprio meio virtual, sem produzir efeitos fora deste ambiente.

Já os crimes cibernéticos impuros, ocorrem quando o agente utiliza a internet como meio executório para a prática de um crime tipificado na nossa legislação, como por exemplo a divulgação de fotografias pornográficas.

Damásio de Jesus e André Estefam, conceituam o referido crime da seguinte forma:

> Os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espeço 'real', ameaçando ou lesando outros bens, não-computacionais ou diversos da informática. (JESUS; ESTEFAM, 2020, p. 223)

Dessa forma, os crimes impuros são aqueles que o agente utiliza do computador e da internet como ferramenta para produzir um resultado que afeta outros bens tutelados que não sejam relacionados aos meios virtuais.

3 LEGISLAÇÃO ATUAL

Com o grande crescimento do meio cibernético, e como consequência o aumento dos crimes virtuais, a Europa se uniu para criar a Convenção de Budapeste, ou Convenção sobre o Cibercrime. Sendo criada em 2001, na Hungria, pelo conselho, está em vigor desde 2004, englobando mais de 20 países e tipificando os principais crimes cometidos na internet.

É importante citar o artigo 22, da Convenção sobre o Cibercrime, uma vez que ela não dita as regras, mas orienta sobre o tema, deixando assim a critério de cada País criar a sua própria legislação sobre o assunto.

> Art. 22 – Competência:
> 1. Cada parte adotará as medidas legislativas e outras que se revelem necessárias para estabelecer à competência relativamente a qualquer infração penal definida em conformidade com os artigos 2º a 11º da presente Convenção, sempre que a infração seja cometida:
> a) no seu território;
> b) a bordo de um navio;
> c) a bordo de aeronave matriculada nessa parte e segundo as suas leis;
> d) por um dos seus cidadãos nacionais, se a infração for punível criminalmente onde foi cometida ou se a infração não for de competência territorial de nenhum Estado.
> 2. Cada parte pode reservar-se o direito de não aplicar ou de apenas aplicar em casos ou condições específicas as regras de competência definidas no nº 1, alínea b à d do presente artigo ou em qualquer parte dessas alienas;
> 3. Cada parte adotará medidas que se revelem necessárias para estabelecer a sua competência relativamente a qualquer infração referida no artigo 24, nº1 da presente convenção, quando o presumível autor da infração se encontre no seu território e não puder ser extraditado para outra Parte, apenas com base na sua nacionalidade, após um pedido de extradição.

> 4. A presente convenção não exclui qualquer competência penal exercida por uma Parte sem conformidade com seu direito interno.
> 5. Quando mais que uma Parte reivindique a competência em relação à uma presumível infração prevista na presente Convenção, as Partes em causa, se for oportuno, consultar-se-ão a fim de determinarem qual é a jurisdição mais apropriada para o procedimento penal. (CONVENÇÃO, 2001, p. 14)

Esse acordo parte do entendimento que para o combate do cibercrime, deve ser realizado um Regime Internacional de mútuo acordo.

No artigo 5º, XXXIX da Constituição Federal Brasileira (CF), é dito sobre o princípio da reserva legal e da legalidade. Sendo assim, as condutas que não estejam previstas em leis não podem ser consideradas como crimes.

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: […] XXXIX - não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal […]. (BRASIL, 1988, n. p.)

Segundo Marco Antônio Marques da Silva (2001), o princípio da legalidade se caracteriza por ser um limite ao poder punitivo do Estado, bem como um limite ao poder normativo, uma vez que impede a criação de tipos penais, com a exceção do processo legislativo regular. Tal princípio é uma consequência direta do fundamento da dignidade da pessoa humana, pois remonta a ideia de proteção e desenvolvimento da pessoa que o tem como referencial.

Até o ano de 2012 não existia qualquer legislação que puniria os crimes virtuais próprios, aqueles voltados contra os dispositivos e os sistemas de informação. Até então, a legislação vigente permitia que os crimes virtuais impróprios pudessem ser punidos, uma vez que consistiam em crimes que já foram tipificados no ordenamento brasileiro, como o fato de o computador ser utilizado como meio para a prática do crime.

Patrícia Peck Pinheiro (2013) cita que diante da evolução tecnológica e da ausência de normas punitivas específicas que protegessem a vítima dos crimes virtuais, já tramitavam no Congresso Nacional, alguns projetos de lei visando a regulamentação desses crimes, dentre eles estão o projeto de Lei n.º 2.126/2011, que institui o marco civil na internet, o projeto de Lei n.º 2.793/2011, de autoria do Deputado Paulo Teixeira e o projeto de Lei n.º 84/1999, de autoria do Deputado Eduardo Azeredo.

Em decorrência de alguns fatos, em que por volta de 2011, ocorreram vários ataques a sites do governo brasileiro, que ficaram instáveis e até saíram do ar, ocasionando o roubo de 36 fotos da atriz Carolina Dieckmann de seus arquivos pessoais e divulgadas na internet por

hackers. O que contribuiu para que as leis específicas sobre o tema fossem aprovadas com urgência, e com o objetivo de preencher as falhas existentes no nosso ordenamento, referentes aos crimes digitais.

Foi no ano de 2012 em que foram sancionadas e promulgadas as leis n.º 12.735, que trata da necessidade de instalação de órgãos especializados para a investigação, e a lei n.º 12.737, pela qual foram incluídos no Código Penal Brasileiro o tipo penal invasão de dispositivo informático e a regra da ação para esse crime. Além da inclusão desses dois dispositivos, a lei alterou a redação de dois outros delitos já existentes, previstos nos artigos 266 e 298 do Código Penal (BRASIL, 1940).

> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
> Pena - detenção, de um a três anos, e multa.
> § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. (Incluído pela Lei nº 12.737, de 2012) Vigência
> § 2º Aplicam-se as penas em dobro se o crime e cometido por ocasião de calamidade pública. (Incluído pela Lei nº 12.737, de 2012) Vigência; […].
> Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:
> Pena - reclusão, de um a cinco anos, e multa.
> Falsificação de cartão (Incluído pela Lei nº 12.737, de 2012) Vigência.
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito. (Incluído pela Lei nº 12.737, de 2012) Vigência Falsidade ideológica. (BRASIL, 1940, n. p.)

Sendo assim, passaram a serem punidas todas as condutas de uso não autorizado de dados de cartões de crédito e débito obtidas de forma indevida, invasão de dispositivos eletrônicos, produção, oferta e venda de propaganda de computadores que permitam a invasão com vírus de internet e obtenção de informações sigilosas ou a violação de comunicações eletrônicas privadas ou segredos comerciais.

Segundo Patrícia Peck Pinheiro (2013), sobre os novos tipos penais, receberão as mesmas penas da invasão aquele que instala uma vulnerabilidade em um sistema de informação para obter vantagem indevida. O usuário de gadgets e dispositivos informáticos comuns estão protegidos contra hackers e pessoas mal intencionadas que abusam de confiança ou buscam intencionalmente devassar dispositivo para se apropriar de dados do computador ou prejudicar o seu proprietário, com a exclusão ou alteração de dados, para que fiquem imprestáveis, ou ainda, informações íntimas e privadas, como fotos, documentos e vídeos. As empresas possuem maior proteção jurídica contra a espionagem digital, pois a obtenção de segredos comerciais e ou informações sigilosas definidas por lei agora também se enquadram na lei.

Ainda de acordo com Pinheiro (2013), a aprovação de dois Projetos de Leis, convertidos em Leis Ordinárias e publicados no Diário Oficial da União, demonstra a preocupação com a vulnerabilidade daqueles que acessam a internet, buscando assim uma tutela Estatal. Contudo, embora a aprovação destas leis represente um primeiro passo para a discussão de tais crimes, punindo agora condutas que até então não estavam tipificadas, ainda há muito para ser discutido em respeito a criminalidade virtual. Para combater este tipo de delito, existem questões a serem resolvidas, além das questões conceituais relacionadas as tipificações dos delitos. Outras inovações jurídicas, como a produção de provas nos crimes digitais, devem ser discutidas a fim de se criar bases legais suficientes para engrandecer o Direito Penal frente esses novos delitos.

3.1 ANÁLISES E DIFICULDADES NA OBTENÇÃO DE PROVAS NOS CRIMES CIBERNÉTICOS

Os avanços tecnológicos e as novas descobertas científicas facilitaram o surgimento de uma nova realidade para o ser humano. O espaço cibernético, novo ambiente social onde a prática de atos e fatos jurídicos independem da existência de um espaço físico, foi o impulsionador que permitiu o surgimento dessa nova realidade (MALAQUIAS, 2012).

Com o desenvolvimento tecnológico, além de permitir o tratamento e processamento automatizado de informações e telecomunicações em vários setores da vida, possibilitou também uma maior diversidade e periculosidade em relação a prática de ilícitos informáticos. De acordo com Crespo (2011, p. 159): “a evolução tecnológica da sociedade supõe uma evolução tecnológica dos ilícitos, tanto nos meios quanto nos objetos”.

Os crimes virtuais, caracterizados pela sua diversidade e periculosidade, geram uma maior dificuldade para averiguação e comprovação, bem como outras questões como a consumação de perícias quanto na identificação da autoria.

No nosso ordenamento jurídico, não há qualquer empecilho na utilização de provas eletrônicas, como é dito no artigo 225 do Código Civil:

> Art. 225. As reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão. (BRASIL, 2002, n. p.)

O Código de Processo Penal também aceita as provas eletrônicas, conforme diz no artigo 231, e logo depois, no artigo 232.

> Art. 231. Salvo os casos expressos em lei, as partes poderão apresentar documentos em qualquer fase do processo.
> Art. 232. Consideram-se documentos quaisquer escritos, instrumentos ou papéis, públicos ou particulares.
> Parágrafo único. À fotografia do documento, devidamente autenticada, se dará o mesmo valor do original. (BRASIL, 1941b, n. p.)

Nos dias atuais as pessoas podem utilizar da assinatura digital ou assinatura eletrônica. Consiste em uma chave privada, um código pessoal que não pode ser reproduzido, a qual evita que o que esteja transmitindo seja lido somente pelo receptor que possua a mesma chave, sendo reconhecida com a mesma validade da assinatura tradicional (PINHEIRO, 2010).

Para cada usuário que navega na internet, lhe é atribuído um número de IP (Internet Protocol), esse é o número que propicia a identificação do usuário na rede, ou a investigação de algum crime que tenha ocorrido, a questão é que esse número só é atribuído ao usuário quando ele está conectado, após o mesmo deligar o modem, o endereço de IP será dado a outro usuário, caso ele não use um IP fixo. Quando solicitado ao provedor de acesso à internet, o número deverá vir acompanhado de data, hora e o fuso horário do sistema, sendo imprescindíveis esses dados, tendo em vista que sem eles fica impossível a quebra de sigilo dos dados.

Após a coleta destes dados, tendo assim a localização do provedor, é necessário o requerimento ao juiz, para que haja a quebra do sigilo de dados telemáticos, para seja informado pelo provedor de acesso quem estava vinculado ao endereço de IP naquele momento em que ocorreu o crime, ou seja, o seu endereço físico.

Segundo Pinheiro (2013), toda investigação tem início com base nas evidências e informações coletadas no meio, sendo ele físico ou virtual. Nos casos dos crimes virtuais, as evidências poderão ser retiradas de qualquer dispositivo eletrônico, celulares, discos rígidos. Isto é, a evidência digital pode ser definida como qualquer informação retirada de um compilado ou deposito eletrônico, através da intervenção humana ou não, em um formato inteligível ao ser humano.

Nas investigações sobre os crimes virtuais, em decorrência da facilidade da adulteração dos dados, as provas deverão passar por perícias técnicas rigorosas para serem aceitas nos processos, de forma a garantir a validade e integridade dos resultados. Esse é o objetivo da computação forense, o de provar os fatos ocorridos de forma mais sucinta o possível.

A computação forense é um tipo de perícia caracterizada pela inspeção cientifica e sistemática em computadores que, através da coleta de provas digitais, busca chegar a

conclusões sobre o caso investigado. É feita uma reconstituição dos eventos encontrados, possibilitando determinar se o computador analisado foi utilizado para a realização ou não de condutas ilícitas.

Segundo Pinheiro (2013), são exemplos de indícios que podem auxiliar na investigação dos crimes digitais os arquivos de imagem de pornografia infantil, mensagens eletrônicas com ameaças e chantagens, arquivos com informações incriminatórias ou dados roubados.

Pelo fato de se desenvolverem e de se consumarem em ambiente virtual, caracterizado de certa forma pela inexistência física do sujeito ativo, uma vez que o criminoso está somente no espaço cibernético, os crimes virtuais são geralmente considerados bastante complexos. Ademais, contribui para essa complexidade a facilidade do perecimento das provas apresentadas para esse tipo de crime, fotografias, vídeos, dados, isto é, a facilidade com que as provas podem ser modificadas, perdidas ou até apagadas da rede (MALAQUIAS, 2012).

Os cibercrimes apresentam dificuldades enormes para sua comprovação. Se por um lado há uma grande facilidade na prática do delito por meio dos computadores, por outro lado a verificação dos vestígios exige uma qualificação técnica específica, que nem sempre está disponível em todos os lugares de consumação dos crimes.

A facilidade de modificação característica dos documentos digitais exige que seja nomeado um perito tecnicamente qualificado para afirmar a autenticidade do documento. Apesar da precisão da computação forense, a coleta de evidências se torna frágil, quando feita equivocadamente, violando disposições de direito material ou princípios constitucionais, podendo tornar a prova ilícita ou invalidá-la (PINHEIRO, 2013).

A produção de prova ilícita pode ser extremamente prejudicial ao processo, na medida em que esse tipo de prova contamina todas as provas dela decorrentes. Sendo assim, todas as provas originárias de uma prova ilícita devem ser retiradas do processo, conforme previsão do Código de Processo Penal no seu artigo 157:

> Art. 157. São inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais. (Redação dada pela Lei nº 11.690, de 2008)
> § 1º São também inadmissíveis as provas derivadas das ilícitas, salvo quando não evidenciado o nexo de causalidade entre umas e outras, ou quando as derivadas puderem ser obtidas por uma fonte independente das primeiras. (Incluído pela Lei nº 11.690, de 2008)
> § 2º Considera-se fonte independente aquela que por si só, seguindo os trâmites típicos e de praxe, próprios da investigação ou instrução criminal, seria capaz de conduzir ao fato objeto da prova. (Incluído pela Lei nº 11.690, de 2008)

> § 3º Preclusa a decisão de desentranhamento da prova declarada inadmissível, esta será inutilizada por decisão judicial, facultado às partes acompanhar o incidente. (Incluído pela Lei nº 11.690, de 2008)
> § 4º (VETADO) (Incluído pela Lei nº 11.690, de 2008)
> § 5º O juiz que conhecer do conteúdo da prova declarada inadmissível não poderá proferir a sentença ou acórdão. (Incluído pela Lei nº 13.964, de 2019) (Vide ADI 6.298) (Vide ADI 6.299) (Vide ADI 6.300) (Vide ADI 6.305). (BRASIL, 1941b, n. p.)

Em decorrência das circunstâncias exigidas para esse tipo de perícia, o maior problema jurídico em relação à produção de provas nos crimes virtuais é o despreparo da polícia investigativa e da perícia. São poucos os profissionais preparados para esse tipo de investigação, por esse motivo, estes deverão ser extremamente capacitados e especializados para lidar com a perícia voltada para investigação dos crimes digitais, de forma a atender exigências técnicas de coleta e guarda a fim de evitar os questionamentos que venham a surgir sobre a identidade da prova e a licitude de sua obtenção (COLLI, 2010).

A respeito da investigação policial e a elaboração do laudo pericial, a capacitação do investigador ou perito está diretamente associada ao sucesso ou não das provas produzidas. Estes profissionais devem estar aptos e treinados para, através da utilização das mais modernas tecnologias, buscar os indícios que possibilitarão a coleta de provas, a preservação do local e das ferramentas e objetos utilizados na prática da conduta ilícita (MALAQUIAS, 2012).

Analisando o ambiente em que o delito foi cometido, os profissionais poderão constatar a existência de vestígios das atividades criminosas praticadas. Malaquias (2012), considerando o envio e um e-mail não autorizado, exemplifica vestígios que podem indicar a prática da conduta infracional quais sejam a indicação da origem de um e-mail, sua autoria, destinatário, adulteração, o itinerário utilizado para se chegar ao destinado final, os endereços virtuais e protocolos de comunicação envolvidos que identificarão o caminho feito pela mensagem na rede de computadores.

Diante da escassez de técnica e recursos humanos preparados no que diz respeito à investigação e punição do criminoso cibernético, os exames periciais transformam-se em um instrumento eficiente na produção de prova no crime cibernético (MALAQUIAS, 2012).

3.2 IDENTIFICAÇÃO DA AUTORIA

O principal objetivo da prova judiciária é a reconstrução da verdade. É a busca pela ligação existente entre os fatos investigados no processo e a realidade histórica, ou seja, a verdade dos fatos tal como realmente ocorreram no tempo e espaço (OLIVEIRA, 2011).

O material probatório colhido durante o processo é de suma importância para o convencimento do magistrado acerca da ocorrência dos fatos objetos da lide. A condenação só poderá ocorrer diante da certeza de culpabilidade, e esta não poderá ser obtida através de suposições, e sim por meio de um conjunto de provas sólido (TAVORA; ALENCAR, 2012).

Para que a sanção penal seja aplicada ao indivíduo que figura como imputado, é necessária a comprovação de que este indivíduo tenha praticado a conduta caracterizada como crime cibernético. Não basta a simples dedução, inferência ou conhecimento superficial sobre a autoria do delito (MALAQUIAS, 2012).

Principalmente em relação aos crimes virtuais, a correta identificação do acusado é uma grande preocupação, para que a pretensão punitiva seja justa e direcionada àquele que realmente cometeu o crime cibernético. Essa preocupação é ainda maior, em relação a identificação do autor, quando se considera, por exemplo, a facilidade que os criminosos têm em se apropriar de senhas e códigos de acesso alheios e utilizá-los para aplicar golpes financeiros ou invadir sistemas por meio dessa identidade (MALAQUIAS, 2012).

A identificação de um indivíduo no "mundo real" e no "mundo virtual" é feita quase da mesma forma. No "mundo real", a identificação de uma pessoa na sociedade corresponde à uma identificação visual, através do reconhecimento das principais características do indivíduo tais como feições, altura, voz e de uma espécie de concretização numérica, que corresponde a um reconhecimento e identificação legal, através do número de um documento como o passaporte ou registro geral. No mundo virtual, a identificação do endereço IP corresponde à concretização numérica, contudo, a grande diferença é que esse número identifica o computador e não uma pessoa.

Toda investigação criminal deve considerar as evidências deixadas pelo criminoso cibernético por intermédio do endereço IP. Outra forma de se obter informações de acesso à rede é através do servidor *proxy*, responsável por armazenar os logs de registro de navegação que identificam os locais acessados pelo usuário, bem como os serviços utilizados, quando a conexão com a rede mundial de computadores é direta. Apesar dessas duas hipóteses investigativas, não há como fazer esse rastreamento, quando o usuário se conecta à rede através de uma conexão indireta, pela qual o internauta fica protegido e usufrui do anonimato on-line para acessar vários conteúdos, utilizando apenas o IP do servidor hospedeiro (MALAQUIAS, 2012).

Apesar da facilidade de rastreamento, permitindo que o computador utilizado para a prática do crime seja facilmente localizado e identificado, a grande dificuldade em identificar o autor decorre da associação feita entre o proprietário do computador e o sujeito que cometeu

o crime. Porém, a identificação do criminoso cibernético não é tão simples assim, quando se leva em consideração que a localização através do endereço IP permite a identificação de um computador e não do autor do delito. Na verdade, a grande dificuldade decorrente da identificação da autoria está em correlacionar o computador e o sujeito que o opera em determinado espaço de tempo.

Pinheiro (2013) diz que a questão da prova de autoria é um dos grandes desafios do direito na era digital. A identificação do criminoso cibernético, de maneira mais inequívoca, só é possível através do uso da biometria que corresponde à utilização de características fisiológicas mensuráveis para autenticar um usuário tais como a impressão digital ou o reconhecimento facial.

Colli (2010) propõe que o sujeito que praticou o crime a partir de um computador somente poderá ser indicado e responsabilizado se houver prisão em flagrante, com o computador ligado. Para ele, essa solução poderá ser utilizada tanto na investigação preliminar, quanto na ação penal dela recorrente.

CONCLUSÃO

O presente trabalho teve como principal objetivo explorar os crimes cibernéticos em face do Direito Penal e Processual brasileiro, sob a visão da legislação atual, apontando suas evoluções e dificuldades, analisando as características decorrentes desse novo ambiente de ocorrência de crimes, que influenciam e dificultam a investigação criminal.

A internet foi um avanço em todos os aspectos que podemos imaginar e vem se expandindo em todas as partes do planeta, com uma grande facilidade de acesso, já que os meios são os mais diversificados, interferindo, inclusive, no comportamento e modo de agir de uma sociedade. Nesse período, nasce um novo espaço e consigo novas práticas delituosas ao passo que a nossa legislação tem que acompanhar essa nova realidade. Assim, são criados os novos posicionamentos dos doutrinadores no que diz respeito a essas novas categorias de crime.

Assim, a recente tipificação de alguns atos criminosos não é suficiente para suprir as dificuldades achadas na resolução de tais crimes. Concluiu-se que o crime cibernético não foi apenas responsável pelo surgimento de novas práticas ilícitas praticadas pelo computador, como também permitiu a violação de bens jurídicos não afetados anteriormente pela prática dos crimes já previstos no ordenamento jurídico brasileiro tais como a informação, dos dados e os sistemas de computadores.

As particularidades obtidas com a ocorrência dos crimes cibernéticos, tais como o dinamismo que estes crimes se concretizam, estão ligadas a investigação probatória. Considerando a importância da prova no processo, bem como os seus elementos. Podemos concluir que ao se considerar os crimes cibernéticos, algumas questões em relação a coleta de provas devem ser analisadas, bem como a necessidade de peritos especializados, a dificuldade na identificação da autoria e a importância da produção antecipada de provas. São de extrema importância os exames periciais, sendo que as investigações necessitam dessas perícias. Dessa forma, diante da falta de técnica e de profissionais preparados, surge a importância de uma especialização dos profissionais que irão atuar nesse tipo de investigação.

Ademais, quando a identificação de autoria, apesar de existir uma facilidade em rastrear um computador onde aconteceu uma prática criminosa, há uma dificuldade em associar o computador ao sujeito ativo que praticou o crime. A utilização da biometria e a prisão em flagrante com o computador ainda ligado seriam alguma das soluções apresentadas para solucionar tal problema.

Portanto, levando em consideração a grande capacidade da facilidade dos meios para se praticar o crime cibernético, a produção de provas antecipadas ganha uma certa importância, levando em consideração a possibilidade de perecimento das provas, fazendo com que seja ainda mais difícil a solução do crime e a identificação dos autores deste delito.

REFERÊNCIAS

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal**: Parte Geral. 26. ed. rev. atual. São Paulo: SaraivaJur, 2020.

BRASIL. Decreto-lei n.º 2.848, de 7 de dezembro de 1940. Código Penal. **Diário Oficial da União**, Rio de Janeiro, RJ, 31 dez. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 26 set. 2021.

BRASIL. Decreto-lei n.º 3.688, de 3 de outubro de 1941. Lei das Contravenções Penais. **Diário Oficial da União**, Rio de Janeiro, RJ, 3 out. 1941a. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3688.htm#:~:text=Fabricar%2C%20importar%2C%20exportar%2C%20ter,a%20ordem%20pol%C3%ADtica%20ou%20social. Acesso em: 24 set. 2021.

BRASIL. Decreto-lei n.º 3.689, de 3 de outubro de 1941. Código de Processo Penal. **Diário Oficial da União**, Rio de Janeiro, RJ, 13 out. 1941b. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 24 set. 2021.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 07 out. 2021.

BRASIL. Lei n.º 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**, Brasília, DF, 11 jan. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 12 out. 2021.

BRASIL. Lei n.º 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. **Diário Oficial da União**, Brasília, DF, 3 dez. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 05 out. 2021.

BRASIL. Lei n.º 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**, Brasília, DF, 24 abr. 2014. Disponível em: planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 24 nov. 2021.

COLLI, Maciel. **Cibercrimes:** limites e perspectivas à investigação policial de crimes cibernéticos. Curitiba: Juruá, 2010.

CONVENÇÃO Sobre o Cibercrime. Budapeste, 23 nov. 2001. Disponível em: https://rm.coe.int/16802fa428. Acesso em: 20 nov. 2021.

CORRÊA, Gustavo Testa. **Aspectos jurídicos da internet**. 5. ed. rev. atual. São Paulo: Saraiva, 2010.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.

FILHO, Olavo. **A problemática em punir os crimes virtuais**. São Paulo, 2017. Disponível em: https://olavofh.jusbrasil.com.br/noticias/488601202/a-problematicaem-punir-os-crimes-virtuais. Acesso em: 15 out. 2021.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

GRECO, Rogério. **Código Penal comentado**. 14. ed. rev. ampl. Niterói, RJ: Impetus, 2020.

JESUS, Damásio Evangelista de; ESTEFAM, André. **Direito Penal:** parte geral. 37. ed. São Paulo: SaraivaJur, 2020.

LEAL, João José. **Direito Penal Geral**: propedêutica penal, teoria da norma penal, teoria do crime, teoria da pena, questões jurídicopenais complementares. 3. ed. rev. atual. Florianópolis: OAB/SC, 2004.

MACHADO, Thiago José Ximenes. **Cibercrime e o crime no mundo informático:** a especial vulnerabilidade das crianças e dos adolescentes. 2017. Dissertação (Mestrado em Criminologia) – Universidade Fernando Pessoa, Porto, Portugal, 2017. Disponível em: https://bdigital.ufp.pt/bitstream/10284/6089/1/DM_Thiago%20Machado.pdf. Acesso em: 01 out. 2021.

MALAQUIAS, Roberto Antônio Darós. **Crime Cibernético e Prova**: a investigação criminal em busca da verdade. Curitiba: Juruá, 2012.

MIRABETE, Júlio Fabbrini; FABBRINI, Renato N. **Manual de Direito Penal**: parte geral. 24. ed. São Paulo: Atlas, 2007.

NUCCI, Guilherme de Souza. **Manual de Direito Penal**. 18. ed. rev. atual. Rio de Janeiro: Forense, 2022.

OLIVEIRA, Eugênio Pacelli de. **Curso de Processo Penal**. 14. ed. rev. atual. Rio de Janeiro: Lúmen Juris, 2011.

PASCHOAL, Janaina Conceição. **Direito Penal:** Parte Geral. 2. ed. atual. Barueri, SP: Manole, 2015.

PINHEIRO, Patrícia Peck. **Direito Digital**. 4. ed. rev. atual. São Paulo: Saraiva, 2010.

PINHEIRO, Patrícia Peck. **Direito Digital**. 5. ed. rev. atual. São Paulo: Saraiva, 2013.

REALE JÚNIOR, Miguel. **Fundamentos de Direito Penal**. São Paulo: Forense, 2020.

SILVA, Marco Antônio Marques da. **Acesso à Justiça Penal e Estado Democrático de Direito**. São Paulo: Juarez de Oliveira, 2001.

TAVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Curso de Direito Processual Penal**. 7. ed. rev. ampl. Salvador: JusPodivm, 2012.

TELES, Ney Moura. **Direito Penal**: parte geral - arts 1º a 120. São Paulo: Atlas, 2004.