FACULDADES FIP MAGSUL

CAIQUE CESAR MARQUES RAMIREZ

CRIMES CIBERNÉTICOS E AS DIFICULDADES INVESTIGATIVAS NA OBTENÇÃO DE INDÍCIOS DE AUTORIA E DA PROVA DA MATERIALIDADE

Ponta Porã – MS

2020

CAIQUE CESAR MARQUES RAMIREZ

CRIMES CIBERNÉTICOS E AS DIFICULDADES INVESTIGATIVAS NA OBTENÇÃO DE INDÍCIOS DE AUTORIA E DA PROVA DA MATERIALIDADE

Trabalho de Conclusão de Curso – TCC apresentado à Banca Examinadora das Faculdades Integradas de Ponta Porã, como exigência parcial para obtenção do título de Bacharel em Direito.
Orientador: Prof. Esp. Marco Aurélio Claro

Ponta Porã – MS

2020

CAIQUE CESAR MARQUES RAMIREZ

CRIMES CIBERNÉTICOS E AS DIFICULDADES INVESTIGATIVAS NA OBTENÇÃO DE INDÍCIOS DE AUTORIA E DA PROVA DA MATERIALIDADE

Trabalho de Conclusão de Curso – TCC apresentado à Banca Examinadora das Faculdades Integradas de Ponta Porã, como exigência parcial para obtenção do título de Bacharel em Direito.
Orientador: Prof. Esp. Marco Aurélio Claro

BANCA EXAMINADORA

_____
Orientador: Prof. Esp. Marco Aurélio Claro
Faculdades Integradas de Ponta Porã

_____
1º Examinador

_____
2º Examinador

Ponta Porã – MS, de _____de_____.

RESUMO

A popularidade da Internet e o desenvolvimento da tecnologia tornaram possível a ocorrência de novos tipos de crimes: os crimes cibernéticos. Tendo em vista que conforme o uso corriqueiro da internet foram surgindo novos delitos, o Direito adaptou-se a essa nova realidade. Os crimes virtuais irão ser abordados no contexto da influência da tecnologia da informação no Direito Penal e também da adaptação na qual o direito passou para se adequar à atualidade. O trabalho disserta sobre os tipos de crimes virtuais, conceito e classificação, busca tecer comentários acerca do Marco Civil da Internet e das demais leis que tratam sobre o assunto no Brasil, haja vista a promulgação de leis específicas acerca do tema terem sido um dos primeiros passos para se combater a esses crimes. Todavia, além da classificação de novos crimes decorrentes da evolução tecnológica, outras questões são afetadas diretamente através das características incomuns dos crimes cibernéticos e que merecem ser discutidas de maneira especial. A rapidez como o crime se perpetua, assim como os bens jurídicos tutelados por esses crimes são particularidades que dificultam e atrapalham a persecução penal, no tocante a produção de provas de autoria e materialidade, daí surge a necessidade de peritos especializados e a necessidade de produção antecipada de prova, questões que são objeto do presente estudo. Desta feita, faz-se necessário um aperfeiçoamento na abordagem investigativa e em todo ordenamento jurídico a fim de se dar punição de forma eficiente e justa aos criminosos digitais.

Palavras-chaves: Crime Cibernético; Prova; Investigação; Autoria; Materialidade

ABSTRACT

The popularity of the Internet and the development of technology have made it possible for new types of crimes to occur: cyber crimes. Bearing in mind that according to the current use of the internet, new crimes have emerged, the Law has adapted to this new reality. Virtual crimes will be addressed in the context of the influence of information technology in criminal law and also in the adaptation that the law has undergone to adapt to the present day. The work dissertates on the types of cybercrime, concept and classification, seeks to comment on the Civil Framework of the Internet and the other laws dealing with the subject in Brazil, given that the enactment of specific laws on the subject were one of the first steps to be taken. combat these crimes. However, in addition to the classification of new crimes resulting from technological evolution, other issues are directly affected by the unusual characteristics of cyber crimes and which deserve to be discussed in a special way. The speed with which the crime is perpetuated, as well as the legal assets protected by these crimes, are particularities that hinder and hinder criminal prosecution, with regard to the production of evidence of authorship and materiality, hence the need for specialized experts and the need for production advance of proof, issues that are the subject of the present study. This time, it is necessary to improve the investigative approach and the entire legal system in order to give punishment efficiently and fairly to digital criminals.

Keywords: Cyber Crime; Proof; Investigation; Authorship; Materiality

SUMÁRIO

INTRODUÇÃO

Com o avanço da tecnologia e as transformações na sociedade contemporânea, a internet foi ampliada em diversas áreas da vida pessoal, social e profissional e tornou-se a principal ferramenta de comunicação, contudo as inovações tecnológicas criaram um ambiente comum para o cometimento de vários crimes, praticados virtualmente.

O surgimento da tecnologia e posteriores evoluções abrem um novo mundo de oportunidades em diversas áreas da vida em sociedade, mas também propiciam práticas de crimes no espaço virtual, cresce a necessidade de a legislação penal ser rápida e eficaz e também atualizar-se com a evolução da sociedade, para que haja a correta tipificação penal e por consequência a punição do agente criminoso.

O estudo pretende expor os aspectos jurídicos da investigação dos crimes cibernéticos e também as dificuldades apresentadas no momento de obtenção de indícios de autoria e da prova da materialidade, seja pela escassez de leis específicas, pela falta de profissionais e delegacias especializadas e a falsa impressão de anonimato na internet, dessa forma a investigação termina sendo morosa e ineficaz, tornando o crime impune por inúmeras vezes, ao não identificar o autor de um crime ou provar a materialidade do fato.

Ademais apesar de serem menos comuns, os crimes de maior potencial ofensivo no ciberespaço ainda não estão legalmente corretos e definidos, e partem de um lugar em que o magistrado deverá se ater de outros métodos de hermenêutica, ficando a vítima à mercê total do entendimento do juiz.

Devido ao pouco material legislativo sobre o tema, ausência de tipificação legal de crimes praticados por meio eletrônico, há uma presente lacuna jurídica que permite a impunidade delitiva e incentiva a sua continuidade. Os agentes que praticam esses crimes por diversas vezes não são identificados, não tem a sua conduta adequada a algum tipo penal ou quando identificados os indícios de autoria e materialidade, pode já ter o seu crime prescrito pelo decorrer do percurso do tempo

Nessa senda, a presente monografia analisará a produção de provas dos crimes cibernéticos ou virtuais a luz da legislação penal específica, visando apresentar as particularidades decorrentes da prática dos crimes digitais. A problemática não se resume apenas à falta de tipificação penal dos crimes cibernéticos praticados, também

surgem outras questões como a dificuldade na identificação da autoria e a produção antecipada de provas, além da presença de profissionais do direito preparados para analisarem o tema e que merecem igual análise e estudo.

Outro problema que surge é a falta de determinação de juízo competente para jugar os delitos virtuais, posto que a lei brasileira possui poucas leis que dissertam sobre o tema, como a Lei do Marco Civil da Internet (Lei 12.965/2014), a popular Lei da Carolina Dieckmann (Lei. 12.737/2012) e a recente alteração no Código Penal pela Lei 13.718/18 que passou a criminalizar a exposição pornográfica não consentida.

A relevância do tema no ordenamento jurídico é nítida, e torna-se cada vez mais necessário estudar sobre as práticas no campo do direito digital e da criminalidade virtual, o direito deve caminhar a passos largos para acompanhar as inovações, da mesma forma que os operadores de direito devem se capacitar para punir esses crimes.

As preocupações, com a garantia da segurança jurídica, em meio a um mundo virtual sem fronteiras visam a proteção de conhecimentos e inovações com a necessidade de regras, regulamentações e leis que tornam viáveis soluções jurídicas para repreensão da conduta criminosa.

Para fins didáticos a presente monografia se desenvolveu em três capítulos, visto que no primeiro capítulo, buscou abordar sobre os antecedentes históricos da internet e sua evolução, assim também a forma como a rede mundial de computadores, surge em um primeiro momento como uma ferramenta de comunicação e após a constante evolução da tecnologia transformou-se em um meio de propagação de condutas criminosas.

No segundo capitulo será explorado o conceito de crime virtual e seus desdobramentos, através da pesquisa de doutrina se verificará toda a dogmática dos crimes virtuais. Durante o capítulo intermediário houve uma análise dos crimes cibernéticos em destaque a algumas conceituações e classificações doutrinárias para esse tipo de crime, além de classificar as ameaças virtuais mais comuns da rede virtual.

E por fim o terceiro e último capítulo, analisará a legislação penal competente ao tema, a competência para julgar os crimes, todavia o principal foco será em apresentar as particularidades na investigação criminal, quanto a produção de provas nos processos que tratam dos cibercrimes e as principais dificuldades existentes na

identificação do agente e na obtenção de provas que comprovem a autoria e a prova da materialidade.

A metodologia utilizada será a exploratória, porque tem objetivo de proporcionar uma familiaridade profunda acerca do tema para torna-lo mais explícito. A função dessa pesquisa é o preenchimento das lacunas que podem aparecer diante do problema discutido no estudo. A escolha dessa forma de pesquisa se justifica pela possibilidade de desenvolver o tema partindo de pesquisa teóricas sobre o assunto, levantamentos doutrinários, bibliográficos, artigos, roteiros, acesso a sites, entre outros recursos que serão explorados.

Para tanto foram utilizadas as obras dos principais autores renomados acerca do tema assim como: Patrícia Peck Pinheiro, Maciel Colli, Marco Antônio Zanellato, Alessandro Baratta, entre outros, também foram consultados artigos publicados.

1. INTERNET E CIBERESPAÇO

A internet é uma praça pública cujo uso coletivo está cada vez mais inserido no cotidiano das pessoas, de acordo com os dados do IBGE, da Coordenação de Trabalho e Rendimento, Pesquisa Nacional por amostra de Domicílios Contínua, em questões tocante ao acesso à internet e uso de meios eletrônicos para uso pessoal, no Brasil em 2017, a internet era utilizada em 74,19% dos domicílios brasileiros.

O meio virtual nasce com a evolução da informática, Pinheiro explica suas origens e explora o processo de desenvolvimento, conforme segue excerto abaixo:

> A informática nasceu da ideia de beneficiar e auxiliar o homem nos trabalhos do cotidiano e naqueles feitos repetitivamente. Tem-se por definição mais comum que a informática é a ciência que estuda o tratamento automático e racional da informação. Entre as funções da informática há o desenvolvimento de novas máquinas, a criação de novos métodos de trabalho, a construção de aplicações automáticas e a melhoria dos métodos e aplicações existentes. O elemento físico que permite o tratamento de dados e o alcance de informação é o computador. (2012, p. 32)

A rede mundial de computadores interliga milhares de máquinas em todo o mundo e é um dos principais avanços no mundo moderno. A internet foi criada pelos Estados unidos durante a Guerra fria, com fins bélicos, para compartilhamento de informações entre o comando, que buscavam uma forma mais rápida e segura de comunicação.

Atualmente assume um outro viés, é utilizada como meio de comunicação, empresarial, publicidade, comércio eletrônico, entre outras formas de uso. A internet pode ser definida como:

> [...] um sistema de rede de computadores interligados a nível global, a qual possibilita a comunicação e a transferência de arquivos de uma máquina a quaisquer outra conectada na rede, possibilitando assim, um intercâmbio de informações sem precedentes na história, de forma rápida, eficiente e sem a limitações de fronteiras geográficas, culminando na criação de novos mecanismos de relacionamento. (CORREA, 2000, p. 135).

Cassanti relata que “a internet é uma grande praça pública, o maior espaço coletivo do planeta”. (2014, p.3)

A tecnologia impacta em diversos aspectos da vida comum, por consequência disso não haveria porque não repercutir também no Direito Penal, que também acompanha o avançar da sociedade e se adapta ao momento atual. A utilização da internet pode ser uma ferramenta de auxílio na prática de condutas criminosas, principalmente ao frequente uso de dispositivos móveis como celulares, notebook e tablets.

Os crimes praticados pela internet e a dificuldade de repressão geram inúmeros debates na sociedade e no ordenamento jurídico pátrio. Com as mudanças advindas do uso da internet, os criminosos levaram os crimes que já aconteciam no mundo real para o virtual e também surgiram novos crimes, gerando insegurança para os usuários que utilizam os recursos e meios oferecidos na rede.

As práticas foram evoluindo e se aperfeiçoando, criando um cenário propício para criminosos e surgimento de novas modalidades de crimes virtuais, assim sendo surgiram novas formas de crimes cometidos no ciberespaço da rede mediante uso do correio eletrônico (e-mails), sites, redes sociais, entre outros. Também presente nas relações de consumo, envolvendo transações eletrônicas, compras que necessitam de dados de cartões de crédito, ou transações bancárias que se utilizam de informações sigilosas, tais quais, senhas, contas correntes e demais mecanismos de segurança.

Legislar sobre a matéria digital e seus crimes cometidos na plataforma é extremamente difícil e muito delicado, isso se dá pela dificuldade em se redigir o novo tipo penal e adequar a prática, porque por muitas vezes corre-se o risco de punir uma pessoa inocente, ou deixar um criminoso impune por ausência de tipificação ou autoria do crime.

Pinheiro aduz que “um computador não traz informações de contexto da situação, tampouco consegue dizer se a conduta foi com ou sem intenção. Um exemplo disso é a tentativa de se tipificar o crime de envio de arquivo malicioso em e-mail” (2012, p.121). Ou seja, um computador não é como uma pessoa que sabe diferenciar uma conduta dolosa ou culposa, também não existem “testemunhas máquinas” para apontar os fatos, o cenário de investigação e julgamento de crimes virtuais é por vezes incerto, conforme será demonstrado no decorrer dessa tese.

O atual capítulo traçará a introdução ao direito digital, a evolução da tecnologia em paralelo ao desenvolvimento da internet e suas atribuições dentro de uma sociedade, assim como tecerá informações de como surgiram as primeiras práticas de crimes virtuais.

1.1 HISTÓRICO DA COMPUTAÇÃO

A informática visa a criação de ferramentas que beneficiem e auxiliem a vida humana nas atividades do dia a dia, em especial aqueles realizados de forma repetida e sequencial. A definição trazida por Pinheiro (2012, p.16) aduz que “a informática é a ciência que estuda o tratamento automático e racional da informação”.

Para informatizar são criadas funções que desenvolvem maquinários novos e criam novos métodos de trabalhos, como a área de tecnologia da informação, a construção de mecanismos que reproduzem ações automáticas além proporcionar melhorias, atualizam os métodos já existentes.

> A necessidade de instrumentos que auxiliassem o homem a processar informações, em apoio a suas funções mentais naturais, não é recente. Pode-se dizer que remonta aos antigos pastores que utilizavam pedras para contabilizar seu rebanho —seria esta a figura representativa dos primórdios do processamento de dados. O primeiro engenho concebido com essa finalidade seria o ábaco. Utilizado por mercadores há mais de 2.000 anos e filho direto das necessidades dos mercantis, o ábaco faz-se com pedrinhas — *calculi* — que, ordenadas segundo a técnica desenvolvida pelos matemáticos de então, auxiliavam a elaboração de cálculos e tarefas de contabilidade que, de outra forma, tomariam muito tempo (PINHEIRO, 2013, p.32)

O homem desde o princípio até a atualidade procura suprir a necessidade de desenvolvimento de utilidades e ferramentas que facilitem as funções comuns diárias. Antigamente os mecanismos criados pretendiam executar operações matemáticas mais complexas, com a premissa de facilitar o trabalho do homem no campo primeiramente e depois no mercado corporativo, daí pode-se citar “ossos de Napier, criado pelo escocês John Napier, onde desdobrou na criação das réguas de cálculo” (PINHEIRO, 2013, p.32).

Ademais em 1642 o filósofo francês Blaise Pascal construiu um engenho mecânico que conseguia somar e subtrair algarismos. Em 1677 o também filósofo, Alemão Gottfried Leibniz construiu sua própria máquina que realizava cálculos. Todavia a Autora Patricia Peck Pinheiro revela que “Somente em 1830, porém, a tecnologia é industrializada e começam a ser fabricadas na Europa máquinas de calcular mecânicas” (2013, p.32).

Após a disseminação nos mecanismos em toda a Europa, no ano de 1834, o norte-americano Charles Babbage cria uma máquina complexa que consegue executar uma sequência de operações matemática de forma predeterminada

A professora Patricia Peck Pinheiro prossegue relatando a história da computação e descreve que:

> Embora nunca tivesse sido finalizada como desejava seu criador, a máquina e as próprias anotações de Babbage lançaram conceitos até hoje fundamentais na computação: a máquina que executa comandos predefinidos — o programa, a interface de entrada/saída e a memória dos cálculos realizados. Em 1847, o matemático britânico George Boole idealiza em sua obra *The mathematical analysis of logic:* being an essay towards a calculus of deductive reasoning uma teoria que aproxima a lógica da matemática, por meio de operadores lógicos (E, OU e NÃO) e um sistema binário de numeração que se utiliza apenas dos algarismos 1 e 0. Tal teoria ficou posteriormente conhecida como Álgebra Booleana e viria a ser amplamente utilizada nos computadores, que ainda tardariam a surgir, pela facilidade em associar os operandos booleanos (1 e 0) a dois estados da corrente elétrica (ligado e desligado). O norte-americano Herman Hollerith concebeu em 1890 uma máquina eletromecânica que lia uma série de dados gravados em cartões perfurados e fez com que o censo daquele ano nos Estados Unidos fosse processado em um terço do tempo do censo anterior. Hollerith mais tarde fundaria a empresa *Tabulating Machine Company*, que hoje é conhecida pelo nome de *International Business Machine* (IBM). (2013, p.32)

Toda essa evolução tecnológica culminou na proliferação de máquinas e instrumentos de fazer cálculos, principalmente em meados de 1930. Porém somente em 1946 deram um passo além das máquinas calculadoras, foi produzido o primeiro computador eletrônico, criado por John Eckert e John Mauchly, da empresa *Eletronic Control*, o projeto recebeu o nome de “ENIAC (*Eletric Numeric Integrator and Calculator),* foi desenvolvido a pedidos do exército para auxiliar e automatizar os cálculos balísticos.

Era um computador baseado em circuitos eletrônicos que operava com lógica binária, composto de 18.000 válvulas” (PINHEIRO, 2013, p.32). O maquinário era tão grande que se situava em diversas salas da Universidade de Pensilvânia, local em que foi criado.

Em 1951, denominada como a segunda geração dos computadores, foi lançado o primeiro computador a ser vendido comercialmente em alta escala denominado de UNIVAC I.

Então nos anos nos anos 60, o computador diminui de tamanho ao substituir as válvulas por transitores, além da dimensão, utiliza do consumo de energia e conseguem aumentar a potência das máquinas. Ainda nos anos 70 “surgem os circuitos integrados, que têm esse nome por reunirem grande número de transistores em uma única peça” (PINHEIRO, 2013, p.32)

Além do exposto acima, nos últimos 40 anos, foram vários fatos somados que contribuíram para a mudança na realidade social, alterando a forma como os homens vivem e se relacionam, a tecnologia mudou tudo, seguem abaixo alguns exemplos que somados a história da computação culminaram na sociedade hodierna.

> Como podemos perceber, além do que ficou exposto acima, nas últimas quatro décadas vários fatos contribuíram para uma profunda mudança na realidade social. Em 1964, Gordon Moore cria a Lei de Moore e revoluciona a produção dos *chips*. O primeiro computador com *mouse* e interface gráfica é lançado pela Xerox, em 1981; já no ano seguinte, a Intel produz o primeiro computador pessoal 286. Tim Bernes Lee, físico inglês, inventa a linguagem HTML (*HyperText Markup Language* ou, em português, Linguagem de Marcação de Hipertexto), criando seu pequeno projeto de World Wide Web (WWW), em 1989; Marc Andreessen cria o *browser Mosaic*, que permite fácil navegação na Internet, em 1993. Em 1996, Steve Jobs lança o iMac. No mesmo ano, dois estudantes americanos, Larry Page e Sergey Brin, em um projeto de doutorado da Universidade Stanford, criam o maior *site* de buscas da internet, o “Google”. Em 1999, um ataque de hackers tira do ar *websites* como Yahoo e Amazon, entre outros. Em 15 de janeiro de 2001 é criada a “Wikipedia”, a primeira enciclopédia *online* multilíngue livre colaborativa do mundo, que pode ser escrita por qualquer pessoa, de qualquer parte do globo, de forma voluntária. Em 23 de outubro de 2001, cerca de um mês depois dos atentados de 11 de setembro, é lançada pela Apple a primeira versão do iPod, de 5GB e tela monocromática, aparelho que revoluciona o mercado de música mundial ao permitir, segundo o seu criador Steve Jobs, o “armazenamento de até 1000 músicas em seu bolso”. Os exemplos são muitos. (PINHEIRO, 2013, p. 33)

Os fatos espelham um longo caminhar para a sociedade digital que conforme passam os anos desenvolve-se de forma rápida, desde a primeira criação de comunicação simultânea, como o telefone, até os últimos lançamentos tecnológicos. A internet encurtou fronteiras e facilitou a comunicação global.

1.2 BREVE RELATO SOBRE A EVOLUÇÃO DA INTERNET

O fenômeno da globalização modificou a forma como a sociedade atual de organiza e funciona em diversos seguimentos. Iniciado em meados da metade do século XX, evidencia o rompimento dos muros erguidos na economia, integrando as sociedades de forma global.

Segundo Damásio de Jesus e José Antônio Milagre (2016, p.14)

> "Vive-se em uma aldeia global, expressão criada por Herbert Marshall McLuhan(1964). Da globalização, surge a sociedade do conhecimento, ou a nova economia, ou, ainda, a sociedade da informação. Vivemos uma economia global e informacional".

A internet se desenvolveu por meio da globalização, de acordo com Conte e Fiorilo (2013, p.24) "a globalização é o processo pelo qual ocorre a integração entre as economias e as sociedades de vários países, sendo que essa permite a transnacionalização de mercadorias, serviços e informações".

Os autores prosseguem explicando que o processo de globalização é um fenômeno "em plena expansão, que verdadeiramente tende a mudar, cada vez mais, a feição de diversos segmentos sociais e científicos, trazendo novos hábitos, novos costumes, novas expectativas, novas possibilidades e novos problemas" (CONTE, FIORILO, 2013, p.25)

A internet surgiu como base de projeto militar norte-americano, com fins bélicos, que projetava uma rede capaz de suportar uma guerra em grande escala e mesmo assim funcionar através dos pontos de conexões ainda que fossem derrubados com um ataque inimigo.

Pode-se conceituar a internet como um grupo de redes de comunicações mundial que interliga milhares de computadores através do protocolo (TCP/IP), que autoriza o acesso das informações e transferência de dados. O ambiente da internet, chamado de ciberespaço, amplia e concerne variedade de recursos e serviços em um mesmo local, uma verdadeira praça pública.

> Tecnicamente, a internet consiste na interligação de milhares de dispositivos do mundo inteiro, interconectados mediante protocolos (IP, abreviação de *Internet Protocol*). Ou seja, essa interligação é possível porque utiliza um mesmo padrão de transmissão de dados. A ligação é feita por meio de linhas telefônicas, fibra óptica, satélite, ondas de rádio ou infravermelho. A conexão do computador com a rede pode ser direta ou através de outro computador, conhecido como servidor. Este servidor pode ser próprio ou, no caso dos provedores de acesso, de terceiros. O usuário navega na internet por meio de um *browser*, programa usado para visualizar páginas disponíveis na rede, que interpreta as informações do *website* indicado, exibindo na tela do

> usuário textos, sons e imagens. São *browsers* o MS Internet Explorer, da Microsoft, o Netscape Navigator, da Netscape, Mozilla, da The Mozilla Organization com cooperação da Netscape, entre outros. (PINHEIRO, 2013, p.33)

O contexto histórico que estava inserido o projeto era a Guerra Fria entre Estados Unidos e União Soviética, que teve início após a Segunda Guerra Mundial em 1945 e culminou na extinção da União Soviética em 1991.

De acordo com BRITO, Auriney (2013. p.21).

> "[...]. No histórico da internet, a ARPANET figura como a principal fonte de criação da internet, mas não como a única. Paralelamente à ARPA, jovens cientistas trabalhavam em projetos em busca do estabelecimento de comunicação entre computadores, quando, a partir da década de 1970, pode-se verificar que várias outras formas descobertas".

No decorrer da década de 1960, o experimento foi financiado pelo departamento de segurança das forças americanas e realizado pelo ARPA (Advanced Research Project Agenc) resultou na primeira forma de comunicação entre computadores, denominada como ARPANET, a Administração de Projetos e Pesquisas Avançados, que daria posteriormente surgimento a internet.

> A origem da internet remonta ao ápice da "guerra fria", em meados dos anos 60, nos Estados Unidos, e foi pensada, originalmente, para fins militares. Basicamente, tratava-se de um sistema de interligação de redes dos computadores militares norte-americanos, de forma descentralizada. À época, denominava-se "Arpanet". Esse método revolucionário permitiria que, em caso de ataque inimigo a alguma de suas bases militares, as informações lá existentes não se perderiam, uma vez que não existia uma central de informações propriamente dita. Posteriormente, esse sistema passou a ser usado para fins civis, inicialmente em algumas universidades americanas, sendo utilizado pelos professores e alunos como um canal de divulgação, troca e propagação de conhecimento acadêmico-científico. Esse ambiente menos controlado possibilitou o desenvolvimento da internet nos moldes os quais a conhecemos atualmente. (PINHEIRO, 2013, p.33)

Inicialmente era utilizada para interligar os centros universitários da Universidade da Califórnia Estados Unidos, nos campos de Los Angeles, Santa Bárbara e da Universidade de Utah. (CONTE, FIORILLO, 2013, p.13)

Em 1970, foi criado o *email*, no qual permitia a troca de textos e mensagens eletrônicas, ganhou grande proporção e popularizou na internet como o primeiro programa de uso geral entre os pesquisadores da época. No final dos anos 70 criaram o *Transmission Control Protocol/Internet Protocol* (TCP/IP), ainda atualmente considerado como o principal protocolo de rede.

Na década seguinte a rede é expandida pelos Estados Unidos, permitindo que houvesse a interligação entre universidades, órgãos militares e o governo, ainda

sendo elitizada e não liberada para o grande público. No ano de 1986, finamente a ARPANET passa a ser chamada de *internet,* nomenclatura que persiste até hoje.

> Posteriormente, esse sistema passou a ser usado para fins civis, inicialmente em algumas universidades americanas, sendo utilizado pelos professores e alunos como um canal de divulgação, troca e propagação de conhecimento acadêmico-científico. Esse ambiente menos controlado possibilitou o desenvolvimento da internet nos moldes os quais a conhecemos atualmente. Entretanto, o grande marco dessa tecnologia se deu em 1987, quando foi convencionada a possibilidade de sua utilização para fins comerciais, passando-se a denominar, então, "Internet". (PINHEIRO, 2013, p.33)

No início de 1990, a Internet foi expandida e evoluiu de maneira jamais vista e sem precedentes, isso se deu por causa de inúmeras criações de recursos que facilitaram o acesso e a transmissão de dados, iniciou nas mensagens do correio eletrônico até os primeiros endereços com terminação ".com", e o acesso ao banco de dados disponibilizados na World Wide Web (www), espaço multimídia. Nessa época ocorreu um verdadeiro amadurecimento no padrão de navegação culminando nos provedores de acesso de conexão ao usuário comum.

Em 1994, a internet alcança o primeiro milhão de usuários, que conseguiu esse feito foi provedor de acesso norte-americano AOL (America On-Line) "em período que se alinha com anos de forte ampliação da microinformática, que se popularizara entre pequenas empresas e residências" (LIMA, 2016, p.25)

A primeira grande revolução da internet, surgiu na década de 1990, foi denominada como a era da internet comercial, momento de rápida expansão, onde os usuários multiplicaram em mais de 50%. Também, nessa época o primeiro grande software popular da internet foi criado, conhecido por Netscape Navigator.

> Com o crescimento da rede, empresas passaram a ter e a fornecer acesso a seus funcionários, aumentando a quantidade de pessoas que utilizavam a internet. Uma característica importante desta época é que era muito complicado publicar algo na internet. O autor precisava conhecer, pelo menos, a linguagem chamada HTML e entender de *softwares* capazes de transmitir a informação do computador pessoal até um servidor. Ou seja, a possibilidade de publicação de qualquer texto era bem reduzida (quer fosse uma explicação científica elaborada ou uma ofensa). (LIMA, 2016, p.25)

As redes sociais deram início a segunda revolução da internet, surgem em 2004, o Orkut e o Facebook, nesse período as publicações e informações estariam distribuídas popularmente.

Expandem-se as possibilidades de conexão entre as pessoas e a facilidade de publicar material na internet. Todos os usuários passam a estar a um clique da publicação de algo. A ambiguidade que trouxe essa ferramenta era a possibilidade das pessoas para utilizar a plataforma tanto para o bem quanto para o mal.

Toda essa evolução acima referida trata-se sobre a conexão por meio de computadores, *desktops* e *notebooks,* até que em 2007 foi criado um dispositivo menor que deu início a era dos smartphones.

> No início de 2007, Steve Jobs surpreende o mundo com o lançamento do primeiro iPhone. Temos um novo gigante passo. O mundo migraria grande parte das atividades de computadores para estes dispositivos menores e, com a melhoria na qualidade da conexão móvel, passaríamos a estar conectados a todo momento, recebendo e enviando informações no carro, no ônibus, na rua, na cama.
> Com a evolução dos *smartphones,* em especial a entrada do sistema Android produzido pelo Google, temos a popularização desses dispositivos, que passaram a ser usados, cada vez mais cedo, por crianças e adolescentes. Nesse momento, vivemos a explosão de aplicativos criados para essas plataformas, com a criação de redes de usuários conectados, transferindo todo tipo de informação. E a história continuará sendo escrita em frente aos nossos olhos. (LIMA, 2016, p.26)

O Brasil que começou com a conexão entre centros universitários brasileiros e americanos. Desde então, seu avanço foi progressivo e contínuo. Com a descoberta de novas tecnologias e com a necessidade de conquistar cada vez mais usuários, a internet alavancou uma desenfreada produção de vários outros equipamentos eletrônicos que conectam o usuário à rede.

1.3 *ORIGEM DOS CRIMES VIRTUAIS*

Sabe-se que a internet encurtou fronteiras e apresenta inúmeros benefícios a diversos setores da vida comum, todavia uma parcela de usuários utiliza a rede para cometer crimes, diante das facilidades trazidas pela tecnologia, os criminosos encontraram uma ferramenta que em sua grande maioria mantém o anonimato, dificultando a identificação do agente e sua localização.

A Internet é rica, e onde há riqueza, existe crime, segundo Eric Schimidt (NERY, AZAMBUJA, 2013, p. 1). A internet ampliou o conceito de espaço físico e limites fronteiriços, alterando o *modus operandi* dos criminosos, houve a migração de pessoas com intuito de fazer da internet um outro ramo para explorar a criminalidade, para obter vantagem das vítimas.

Nesse cenário, a situação no Brasil aumentou no Ano de 2019 um percentual de 110%, sendo registradas uma média de 366 crimes cibernéticos por dia, de acordo com os dados comunicados pela associação Safernet[1], é um número assustador o alto índice de delitos cometidos na plataforma.

O direito busca acompanhar a evolução da sociedade, ele se renova a medida dos fatos novos, e necessita criar mecanismos de direitos e deveres aos cidadãos. Diante das necessidades apresentadas pelas inovações, a tecnologia inserida no cotidiano das pessoas, fez-se inevitável o Direito tutelar as relações provenientes do ambiente virtual.

Os crimes cibernéticos são aqueles praticados por meio do uso da tecnologia, tal como computadores, internet, celulares, entre outros. Por terem uma definição ampla, uma conduta virtual pode atingir o equipamento de um só usuário e também redes completas, como nos ambientes corporativos, organizações, entidades e órgãos públicos.

Segundo Moisés de Oliveira Cassanti (2014, p.17):

> "[...] a partir do segundo semestre do ano de 2011 acompanhamos um aumento muito expressivo dos chamados dispositivos móveis como celulares, smartphones e tablets. Com isso, os ataques virtuais que antes eram restritos aos computadores estão migrando para as plataformas móveis"

[1] A SAFERNET BRASIL é uma associação civil, de direito privado, sem fins lucrativos e econômicos, de duração ilimitada e ilimitado número de membros, sem vinculação político partidária, fundada em 20 de Dezembro de 2005, com sede e foro no município de Salvador, capital do Estado da Bahia.

Com a tecnologia evoluindo as práticas criminosas foram acompanhando essa evolução, de acordo com as inovações apresentadas, mostram-se cada dia mais preparados para a prática e a violação dos softwares de segurança desenvolvidos com a finalidade de dar uma maior proteção ao usuário.

Nas palavras de Auriney Brito (2013. p.18).

> "[...] não há instituições financeiras sem computadores e internet; a maioria dos serviços públicos necessita de uma central informatizada; grande parte das grandes empresas- senão todas elas - possui bancos de dados para controle orçamentário e contábil, de estoques e de clientes. Os pequenos empreendimentos certamente estagnarão ou desaparecerão se não se adequarem à realidade em estudo".

Os primeiros crimes virtuais documentados pela comunidade cientifica internacional, aconteceram no século XX, em 1960 onde se obteve as informações iniciais sobre os crimes realizados virtualmente, na ocasião em que agentes de má fé manipulavam e boicotavam os sistemas de computadores da época.

> O surgimento dos crimes informáticos, que começou na década de 1960, época em que apareceram na imprensa e na literatura científica os primeiros casos de uso do computador para a prática de delitos, constituídos, sobretudo, por manipulações, sabotagens, espionagem e uso abusivo de computadores e sistemas, denunciados em matérias jornalísticas. Somente na década seguinte é que se iniciariam os estudos sistemáticos e científicos sobre essa matéria, com emprego de métodos criminológicos, analisando-se um limitado número de delitos informáticos que haviam sido denunciados, entre os quais alguns casos de grande repercussão na Europa por envolverem empresas de renome mundial. A partir de 1980, o aumento de ações criminosas que passaram a incidir em manipulações de caixas bancárias, pirataria de programas de computador, abusos nas telecomunicações etc., revelando vulnerabilidade que os criadores do processo não haviam previsto. (BUENO, James Nogueira, COELHO, Vânia Maria Bemfica Guimarães, Crimes na internet. Disponível em <https://www.fadiva.edu.br/documentos/jusfadiva/2008/12.pdf> Acesso em 26 de set 2020.)

Damásio de Jesus e José Antônio Milagre (2016, p.20), acerca da origem do primeiro delito informático registrado, aduzem que:

> A doutrina diverge acerca do primeiro delito informático cometido. Para alguns, o primeiro delito informático teria ocorrido no âmbito do MIT (*Massachusetts Institute of Technology*), no ano de 1964, onde um aluno de 18 anos teria cometido um ato classificado com cibercrime, tendo sido advertido pelos superiores. Outros ainda referenciam o primeiro caso de que se tem notícia sobre *hacking* no ano de 1978, na Universidade de Oxford, onde um estudante copiou de uma rede de computadores uma prova. Uma invasão seguida de uma cópia. Até essa data não existia lei sobre crimes informáticos nos Estados Unidos. A Flórida, no mesmo ano, foi o primeiro Estado americano a formular leis sobre informática.

A figura do Hacker, surge em 1970, estabelecida como a prática de violação dos sistemas de furtos de softwares e em 1980 a criminalidade virtual aumentou, e

deu início a inúmeras outras formas delituosas, crimes como a pirataria, invasão de sistemas, pedofilia, furto de dados, entre outros.

O Brasil somente começou a se interessar sobre o tema nas últimas décadas, por causa a vulgarização dos usuários no uso da tecnologia, em 1988 a Constituição Federal trouxe dispositivos sobre direito informático e também a legislação penal competente do Estado.

> Atualmente ainda sem a tipificação pertinente e com a facilidade de acesso a redes mundiais de computadores em nosso ordenamento jurídico não são satisfatórios para denominar os crimes realizados contra o computador ou através dele por meio as novas particularidades criminosas que aparecem e que necessitam serem definidas em leis especial, para a proteção do sistema jurídico. O computador ou sistema de informática é um mecanismo parecido como outros, arma de fogo, manuseados por criminosos para auxiliar na prática de um crime. Compete ao Estado amparar os novos atributos e danos aos variados bens e interesses que se originaram com a gradativa informatização das práticas particulares e gerais expandidas na coletividade. (CARNEIRO, 2012, p.32 e 35)

1.4 ESPAÇO VIRTUAL

O ciberespaço ou espaço virtual é difícil de ser explorado para fins de definição de seu conceito, pois não há como definir um espaço onde não há barreiras físicas, não existe um limitador ou representação material, todavia os efeitos produzidos adentram as esferas dos fatos, no mundo real.

A palavra espaço é definida como extensão ideal, sem limites, que contém todas as extensões finitas e todos os corpos ou objetos existentes ou possíveis. O ciberespaço por sua vez cuida-se de um espaço destinado em sua maioria para a comunicação, onde não há um lugar definido.

O principal ambiente do espaço virtual é a internet, meio popular de utilização, todavia os demais dispositivos eletrônicos como satélites, smartphones, redes de informação, entre outros meios também são considerados serviços de comunicação. Silvana Drumond Monteiro conceitua ciberespaço como:

> Ciberespaço é definido como um mundo virtual porque está em presente potência, é um espaço desterritorializante. Esse mundo não é palpável, mas existe de outra forma, outra realidade. O ciberespaço existe em um local indefinido, desconhecido, cheio de devires e possibilidades. Não podemos, sequer, afirmar que o ciberespaço está presente em nossos computadores, tampouco nas redes, afinal onde fica o ciberespaço? Para onde vai todo esse “mundo” quando desligamos nossos computadores? É esse caráter fluido do ciberespaço que o torna virtual. (2004, p.35)

O escritor William Gibson foi o criador da expressão, ele define ciberespaço como “o conjunto de rede de computadores na quais todo o tipo de informação é circulada, um espaço existente no mundo da comunicação” (2003, p.67).

Com o desenvolvimento da tecnologia, o ciberespaço é um novo lugar para acesso a dados. Uma nova tecnologia ou método que absorve todos os outros recursos e possui recursos inimagináveis. Trata-se de um novo espaço pouco conhecido e com muitos desafios e incertezas. Um espaço em branco, não explorado por completo ou sem existência abstrata é um lugar construído no sistema.

Assim, o espaço virtual é um local de criação de expressões culturais, nomeado de cultura digital, também destinado para comercialização, exploração de campos econômicos e sociais. Inserido nesse aspecto, e considerando os avanços tecnológicos, antes da falta de representação, indicam momentos de dificuldade crescente de cognição, linguagem e produção de conhecimento.

2. CRIMES VIRTUAIS

No campo dos avanços tecnológicos, no contexto da informática e a sua utilização por pessoas, surge a necessidade da tutela desses novos direitos, o Direito Digital consiste na evolução do próprio Direito, abrangendo todos os princípios fundamentais e institutos que estão vigentes e são aplicados até hoje, assim como introduz novos institutos e elementos para o pensamento jurídico, em todas as suas áreas.

O principal desafio tratando-se de crimes informáticos é o fato do Código Penal ser muito antigo e embora tutele a maioria dos delitos informáticos, omite questões em que a informática deveria ter salvaguardado o bem jurídico pelo Direito Penal.

O desenvolvimento da tecnologia iniciou uma nova sociedade denominada como “era da informação”, as pessoas são dependentes da informática, parâmetro e ambiente que servem como base nas relações jurídicas.

Quando o Direito após um processo de evolução passou a reconhecer outros valores penalmente relevantes, começaram as discussões acerca de normas para proteger os cidadãos do uso perverso e mal-intencionado das novas tecnologias.

Considerando que o direito apenas deve agir para a preservação dos bens jurídicos mais relevantes e imprescindíveis às relações sociais e também precisa intervir minimamente na vida do cidadão, aprovar uma legislação que tipificasse crimes cibernéticos não foi fácil, decorreu de um longo processo de evolução do direito. Sobre o processo de evolução segue os excertos abaixo da doutrina de Damásio de Jesus e José Antônio Milagre:

> Em tal contexto, em que pese a sabida proteção oferecida aos bens jurídicos tradicionais, era preciso proteção diante dos delitos cometidos em face de bens jurídicos informáticos. Novas figuras delitivas no Código Penal, embora no nosso sentir não resolvam o problema da falta de estrutura investigativa, sem dúvida alguma eram clamadas por autoridades e operadores do Direito. E elas surgiram. De fato, é inegável que onde há relevância econômica deve haver relevância jurídica, e é esta a tutela que se apresenta, a proteção à incolumidade de informações, bancárias, financeiras, dentre outras informações geradas e tratadas por pessoas físicas e jurídicas. Sistemas informáticos processam ou tratam dados eletrônicos, geram significado e informações. Logo, são merecedores da tutela penal, pois informação é bem precioso. Como salienta Ferreira Lima (2011, p. 6), diante da evolução tecnológica existe uma predisposição social em reconhecer bens jurídicos informáticos e, dentre os que mais se sobressaem, temos o sigilo e a segurança de dados e informações eletrônicas. Para a autora, é tal juízo de reprovação (violação a dados e a informações privadas) que move o Direito

> Penal. De fato, tal juízo de reprovação existia, mas foi preciso que uma pessoa pública, atriz popular, fosse vítima de um suposto crime informático para que o legislativo finalizasse uma discussão de mais de 10 (dez) anos no Congresso Nacional, com a aprovação da Lei n. 12.737/2012, sancionada em 30 de novembro do mesmo ano. (2013, p.123)

A informática e o uso dos dispositivos tecnológicos foram elevados ao *status* de valores jurídicos fundamentais das relações sociais de uma sociedade dependente da tecnologia da informação, devendo ser protegidos. Por isso os “crimes virtuais” no Direito Penal, tutela a informática, a privacidade e a integridade dos dados informáticos.

2.1 CONCEITO E CLASSIFICAÇÃO

O Decreto-Lei nº 3.914 de 09 de dezembro de 1941 Lei de Introdução do Código Penal (decreto-lei n. 2.848, de 7 de dezembro de 1940) e da Lei das Contravenções Penais (decreto-lei n. 3.688, de 3 outubro de 1941), diz em seu art. 1º que:

> "Art. 1º Considera-se crime a infração penal que a lei comina pena de reclusão ou de detenção, quer isoladamente, quer alternativa ou cumulativamente com a pena de multa; contravenção, a infração penal a que a lei comina, isoladamente, pena de prisão simples ou de multa, ou ambas, alternativa ou cumulativamente (BRASIL, 1941)

Pressupõe pela leitura do artigo acima que qualquer infração penal que comine em pena, estaremos diante de um crime, considera-se o critério legal. Todavia no Código Penal atual o conceito de crime não está expresso, como nas legislações anteriores, ficando a cargo dos doutrinadores o definirem e conceituarem. (MIRABETE, 2006, p. 42)

Crime em um aspecto material pode ser considerado toda e qualquer ação ou omissão humana que possa lesionar ou expor a risco bens jurídicos tutelados pelo Direito Penal. Neste critério o que é levado em conta é a relevância o mal alcançado pela conduta do agente. É, portanto, considerado o crime como conduta legítima toda a vez que tiver elo a provocação de dano ou ameaça a bem jurídico com relevância jurídico-penal**.**

O Crime formal parte do princípio no qual crime é uma conduta que viola a lei penal incriminadora, constitui em todo ato ou fato que a lei proíbe e impõe pena, ainda pode-se conceituar como todo fato que o ordenamento jurídico associa a pena como consequência legítima.

Guilherme de Souza Nucci disserta sobre o aspecto analítico e conceitua como:

> Crime trata-se de uma conduta típica, antijurídica e culpável, vale ressaltar uma ação ou omissão ajustada a um modelo legal de conduta proibida (tipicidade), contrária ao direito (antijuridicidade) e sujeita a um juízo de reprovação social, incidentes sobre o fato e seu autor, desde que presentes a imputabilidade, consciência potencial de ilicitude e exigibilidade e possibilidade de agir conforme o direito. (2016, p.202)

Para se falar em crime cibernético parte-se do princípio de que ele é um crime assim como outros, também cometido da mesma forma, exigindo sempre uma conduta típica, antijurídica e culpável, porém há diferenças, no tocante ao campo de

atuação, pois o criminoso estabelece contato com a vítima mediante um dispositivo eletrônico (computador, telefone celular, etc).

Em que pese a nomenclatura pareça algo simples e superficial, ao tratar sobre a matéria, surge uma problemática, posto que não há unificação acadêmica e doutrinária acerca do nome, as consequências dessa divergência paira sobre os resultados ineficazes na sua aplicação no caso concreto.

Mas para que é necessária uma harmonia ao *nomen juris* dado à matéria? Para que toda pesquisa dedicada sobre o tema seja embasada de uma única fonte, a mesma terminologia jurídica para todos os casos, como é o caso do crime de estupro, fraude, sequestro.

Assim, sendo os crimes virtuais recebem inúmeras nomenclaturas, podem ser chamados de crimes eletrônicos, crimes digitais, cyber crimes, crimes cibernéticos. Dá-se esses nomes a atividade na qual um computador ou rede é acessado por um agente com fins criminosos. Esses crimes podem ser caracterizados de acordo com a sua forma de cometimento, assim sendo há crimes, virtuais que são cometidos tendo o computador como instrumento para se executar a infração e outros crimes que possui o aparelho eletrônico em si, que é danificado ou violado de alguma forma.

O crime cibernético “é taxado como o mais apropriado e mais utilizado no meio policial, embora informalmente sejam utilizados os nomes ‘crimes digitais’, ‘crimes eletrônicos’, ‘crimes informáticos’, ‘e-crimes’, ‘crimes virtuais’, dentre outros”. (REDE EADSENASP, 2015).

A resposta para a pergunta sobre o que é crime cibernético encontra-se de forma bem clara e expressa no domínio do site Norton.com, explica que:

> O crime cibernético é todo crime que é executado online ou principalmente online. Isso pode incluir desde os roubos de identidade e outras violações de segurança mencionadas acima a crimes do tipo "pornografia de vingança", "cyberstalking", assédio, bullying e até mesmo exploração sexual infantil. Os terroristas colaboram cada vez mais pela Internet, transferindo esses terríveis crimes para o espaço cibernético.(NORTON, Como reconhecer e se proteger contra o crime cibernético, Disponível em < https://br.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html> acesso em 20 de dezembro de 2020)

Toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material. (ROQUE, 2007, p.25)

As recomendações da *Organization for Economic Cooperation and Development* (OECD), de 1986, conceituam crime eletrônico no seguinte sentido:

“qualquer comportamento ilegal, aético ou não autorizado envolvendo processamento automático de dados e, transmissão de dados, podendo implicar a manipulação de dados ou informações, a falsificação de programas, o acesso e/ou o uso não autorizado de computadores e redes”.

Acrescenta Fabrízio Roza *apud* Damásio de Jesus e José Antônio Milagre (2013, p. 116), sobre o conceito de crimes cibernéticos.

> Ao tratar da denominação envolvendo crimes cibernéticos, bem pontua que “Klaus Tiedemann fala em ‘criminalidade de informática’ para designar todas as formas de comportamentos ilegais ou, de outro modo, prejudiciais à sociedade, que se realizam pela utilização de um computador. Aqui, Tiedemann engloba, por um lado, os problemas da esfera privada do indivíduo que possa ser ameaçada pela memorização, interconexão e transmissão informática de dados, e, por outro lado, os atentados ao patrimônio cometidos através de computadores ou sistemas. Kohn utiliza *computer criminals* para designar seus praticantes. Jean Pradel e Cristian Feuliard referem-se a ‘infrações cometidas por meio de computador’. Há ainda quem prefira a expressão ‘crimes de computador’, ‘cybercrimes’, ‘computer crimes’, ‘computing crimes’, ‘delito informático’, ‘crimes virtuais’, ‘crimes eletrônicos’ ou ainda ‘crimes digitais’, ‘crimes cibernéticos’, ‘infocrimes’, ‘crimes perpetrados pela Internet’, denominações distintas, mas que, no fundo, acabam por significar basicamente a mesma coisa”.

Na mesma linha, trazendo um conceito amplo e claro sobre os crimes cibernéticos Patricia Peck Pinheiro discorre dizendo que:

> Os crimes digitais podem ser conceituados como sendo as condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas a interceptação de comunicações, modificações de dados, infrações a direitos de autor, incitação ao ódio e descriminação, escárnio religioso, difusão de pornografia infantil, terrorismo entre outro. (2013, p. 121)

Nesta senda, relevante destacar as importantes lições do professor Crespo (2011, p. 63) sobre o conceito de crimes virtuais:

> “A simples utilização de um computador para a perpetração de um delito como um estelionato não deveria ser – repita-se – com precisão técnica, considerada um crime informático. Ocorre, todavia, que não só autores, mas também as mídias em geral, convencionaram denominar crimes informáticos qualquer delito praticado com o uso da tecnologia, seja ela o instrumento da conduta, seja o objeto do ilícito. Destarte, apesar de não ser a mais técnica, a nosso ver, é impossível ignorá-la, dada sua particular popularidade acadêmica e, por que não, social, vez que mesmo a mídia em geral passou a se valer dessa mesma classificação”.

De acordo com os ensinamentos das doutrinas acima expostas, crime cibernético pode ser conceituado como todo e qualquer fato típico, antijurídico e culpável cometido por intermédio da tecnologia da informação ou contra ela. Advém do direito digital, que pressupõe um conjunto de normas e princípios sobre a atividade da tecnologia da informação.

Assim sendo, o crime cibernético, é um ato típico e antijurídico, cometido através da informática em geral, ou contra um sistema, dispositivo informático ou rede de computadores. Em verdade, pode-se afirmar que, no crime informático, a informática pode tanto ser o bem ofendido quanto o meio utilizado para a ofensa a bens já protegidos pelo Direito Penal.

O rol dos crimes cometidos por meio eletrônico, não é taxativo, a sua lista é longa e vasta e a cada dia se renova. Dentre eles, pode-se citar: os crimes contra a honra (injúria, calúnia e difamação), crimes de furtos, estelionatos, fraudes com cartão de crédito, desvio de dinheiro de contas bancárias, entre outras formas.

As ferramentas utilizadas para a prática desses delitos são inúmeras cita-se a título de exemplo as seguintes formas: interceptação de comunicações, alteração de dados, pornografia infantil, terrorismo.

A informática é a ciência que se dedica ao tratamento da difusão das informações utilizando de computadores e demais dispositivos de processamento de dados. E, neste sentido, a boa prática impõe que os tipos sejam nominados de acordo com o bem jurídico que visam proteger.

Igual ao crime convencional, o crime virtual pode assumir diversas facetas, assim como poderá ocorrer em qualquer lugar ou tempo. Inserido em um contexto tecnológico, qualquer infração penal que o autor utilizar de recursos tecnológicos para praticar o delito será considerado e tratado como “crime cibernético”.

A princípio o crime eletrônico é um crime de meio, ou seja, utiliza-se de um meio virtual. Não é um crime de fim por natureza porque é um crime em que sua modalidade “só ocorra em ambiente virtual, à exceção dos crimes cometidos por *hackers*, que de algum modo podem ser enquadrados na categoria de estelionato, extorsão, falsidade ideológica, fraude, entre outros” (PINHEIRO, 2013 p.121).

A professora Patrícia Peck Pinheiro (2013, p. 150) assim aduz:

> “Não é crime-fim por natureza, ou seja, o crime cuja modalidade só ocorra em ambiente virtual, à exceção dos crimes cometidos por *hackers*, que de algum modo podem ser enquadrados na categoria de estelionato, extorsão, falsidade ideológica, fraude, entre outros”.

Todavia, na doutrina há discussões que entendem diversamente ao exposto acima. Os estudos revelam que o crime virtual é um crime-meio, mas que ao longo do tempo está evoluindo para um crime-fim, por isso a tipificação de alguns crimes informáticos próprios, foram editados com a promulgação das Leis n. 12.735/2012 e n. 12.737/2012.

Ademais, trata-se de um tipo comum, o crime-fim pode ser cometido por qualquer pessoa, não só por *hackers*. Fato é que a maior parte dos crimes eletrônicos está relacionada a delitos em que o meio para a realização da conduta é virtual, mas o crime em si não. Segue a explicação:

> A exemplo, tem-se como crimes mais comuns praticados na rede o estelionato e a pornografia infantil e os ataques mais comuns os praticados por meio de vírus de computador ou *malware*, seguido de invasão de perfis nas redes sociais e por ataques de *phishing*. Já os crimes cibernéticos mais raros (porém crescentes) continuam sendo aqueles causados por códigos maliciosos, negação de serviço, dispositivos roubados, sequestrados e roubo de informações privilegiadas. Quando combinados, esses fatores são responsáveis por mais de 78% dos custos anuais com crimes cibernéticos para as organizações. Como visto, em que pese o Direito Penal já proteger certos bens jurídicos agredida via informática, fato é que os dados e a segurança dos sistemas e redes informáticos clamavam por uma proteção específica. (PINHEIRO, 2013, p.152)

Dessa forma o meio de materialização do crime pode ser no espaço cibernético, e em certos casos, uma grande parcela dos crimes cometidos na rede ocorre também fora dela, a internet é um modo, um agente facilitador, isso ocorre principalmente pela falsa sensação de anonimato.

2.2 CLASSIFICAÇÃO DOS CRIMES INFORMÁTICOS

O Direito da Informática pode estar presente em diversas esferas do Direito, na seara do Direito Civil a Informática é explorada em normas, regulamentações e entendimentos jurídicos que dissertem sobre as relações privadas estabelecidas através da tecnologia, já no Direito Penal o englobado de normas, regulamentos e entendimentos jurídicos tem objetivo de repreender os fatos criminosos que atentem contra bens da informática.

A melhor doutrina classifica os crimes virtuais em próprios, impróprios e mistos, mediatos ou indiretos.

Crimes informáticos próprios ou puros são aqueles em que o bem jurídico ofendido é diretamente o campo da tecnologia da informação. Nestes delitos, a legislação penal apresenta lacunas, e a luz do princípio da reserva penal, muitas práticas delituosas não seriam enquadradas criminalmente;

> Os Delitos de Informática Próprios ou Puros são aqueles em que ambos o meio e o fim pretendido pelo infrator encontram-se no próprio campo da informática. Trocando em miúdos, ele utiliza-se da informática para danificar ou atingir elementos integrantes da própria informática, como os softwares, hardwares e os dados contidos em quaisquer chips, seja contra um único indivíduo ou contra vários ou ainda contra outros entes, como a própria Internet. Exemplo clássico deste tipo de delito é o acesso não autorizado a um sistema informático utilizando-se de um computador, objeto de estudo do professor Túlio, demonstrando, inclusive, que este delito ainda não se encontra tipificado ordenamento jurídico brasileiro. (TRINKEL, G, 2010, p.16)

Crimes informáticos impróprios ocorrem quando a tecnologia da informação é o meio utilizado para agredir bens jurídicos que já são consagrados e protegidos pelo Código Penal brasileiro. Dessa forma, a legislação criminal brasileira já é suficiente para a sua reprimenda, pois grande parte das condutas realizadas encontra correspondência em algum dos tipos penais;

Os casos mais comuns que se enquadram nestes tipos de delitos são os crimes contra a honra em sites de relacionamentos, como o “Orkut", em que o infrator se utiliza destes como meio para difundir a sua ofensa mais rápida e eficientemente. (TRINKEL, G, 2010, p.16)

Crimes informáticos mistos são crimes complexos onde há proteção de mais de um bem jurídico, além da proteção da inviolabilidade dos dados, a legislação protege outro bem jurídico. Ocorre a existência de dois tipos penais distintos, no qual cada dispositivo protege um bem jurídico; Exemplo dessa classificação é o crime de

acesso não autorizado a sistemas computacionais do sistema eleitoral, previsto no inciso Vll do artigo 67 da Lei 9.504/97, da leitura que se segue:

Art. 67. Obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou contagem de votos.(BRASIL, 1997)

Crime informático mediato ou indireto por sua vez são aqueles delitos praticados para que ocorra e seja consumado ao final outro delito não informático. Nesse caso o delito informático é cometido como meio para a prática de um delito-fim de ordem patrimonial, muito comum nos crimes cibernéticos. Por exemplo no caso do agente infrator que captura dados bancários e os utiliza para retirar valores da conta corrente da vítima. Pelo princípio da consunção, o agente só será punido pelo delito-fim (furto).

> Por fim há os Delitos Informáticos Mediatos ou indiretos, sendo a utilização do computador um mero meio para a obtenção de um fim específico e diverso do campo da informática, como, por exemplo, a invasão de um sistema informático bancário para transferir fundos monetários de uma conta a outra sem o consentimento do dono da conta bancária. Neste caso ter-se-ia apenas o crime de furto, porém não se confundiria com o delito informático impróprio pelo fato de ter havido, neste caso, a violação direta de dados informáticos, porém sendo de inferior gravidade frente ao delito patrimonial realizado. (TRINKEL, G, 2010, p.16)

Cumpre observar duas categorias indicadas pelo professor Marcelo Crespo que categorizam os crimes cibernéticos: como crimes digitais próprios (ou puros) e crimes digitais impróprios (ou mistos):

> Crimes digitais próprios ou puros (condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os sistemas informáticos e os dados. São também chamados de delitos de risco informático. São exemplos de crimes digitais próprios o acesso não autorizado (hacking), a dissemina-ção de vírus e o embaraçamento ao funcionamento de sistemas; e Crimes digitais impróprios ou mistos (condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os bens jurídicos que não sejam tecnológicos já tradicionais e protegidos pela legislação, como a vida, a liberdade, o patrimônio, etc). São exemplos de crimes digitais impróprios os contra a honra praticados na Internet, as condutas que envolvam trocas ou armazenamento de imagens com conteúdo de pornografia infantil, o estelionato e até mesmo o homicídio. (CRESPO, 2015, p.125)

Ademais, cumpre destacar, acerca das inovações legislativa, pois, que os novos tipos penais previstos na Lei n. 12.737/2012 são crimes afetos, via de regra, à categoria de crimes informáticos próprios, onde o bem jurídico protegido é a segurança dos dispositivos e dados informáticos.

2.3 SUJEITO ATIVO DO CRIME CIBERNÉTICO

Antigamente, o perfil de criminoso digital estava relacionado diretamente ao conceito de *cracker*, pessoa com conhecimentos técnicos de um computador ou dispositivos eletrônicos, conhecedora de redes, programações, protocolos, dentre outras habilidades.

Todavia o cenário foi modificado, atualmente a realidade é que não tem como de fato traçar um perfil de criminoso, posto que grande parte dos crimes digitais se concretizam em razão da falta de conhecimentos dos usuários, falta de preparação das autoridades investigativas além da banalização e difusão das técnicas e ferramentas para aplicação de golpes.

Os criminosos digitais, em sua maioria, não praticariam crimes do mundo real, porém interessam-se pela prática delituosa virtual, amparados pela falsa sensação de anonimato.

Mauro Marcelo Lima e Silva acerca do sujeito ativo dos crimes virtuais afirmou que:

> "Geralmente, os criminosos são de oportunidade e os delitos praticados por agentes que, na maioria das vezes, têm a sua ocupação profissional ligada à área de informática. O perfil do criminoso, baseado em pesquisa empírica, indica jovens, inteligentes, educados, com idade entre 16 e 32 anos, do sexo masculino, magros, caucasianos, audaciosos e aventureiros, com inteligência bem acima da média e movidos pelo desafio da superação do conhecimento, além do sentimento de anonimato, que bloqueia seus parâmetros de entendimento para avaliar sua conduta como ilegal, sempre alegando ignorância do crime e, simplesmente, 'uma brincadeira'. preferem ficção científica, música, xadrez, jogos de guerra e não gostam de esportes, sendo que suas condutas geralmente passam por três estágios: o desafio, o dinheiro extra e, por fim, os altos gastos e o comércio ilegal". (SILVA, M. Os crimes digitais hoje, Conjur, 2000. Disponível em: <https://www.conjur.com.br/2000-set-02/policia_revela_perfil_criminoso_internet/>.Acesso em 20.out.2020)

Dentre as nomenclaturas existentes nas doutrinas, podemos citar:

Hackers significa Fuçador. Expressão que surgiu nos laboratórios do MIT (*Massachusetts Institute of Technology*). Sendo uma pessoa que tenha grande conhecimento sobre tecnologia e que faça invasões a dispositivos eletrônicos.

Carders são aqueles agentes estelionatários especializados em fraudes com cartões.

Crackers seriam os verdadeiros criminosos dentro da rede, pois tem má-fé. Utilizam seus conhecimentos de tecnologia para fins criminosos.

Phreakers são os “*hackers* da telefonia”, capazes de realizar interceptações, paralisar serviços e até mesmo utilizar a telefonia em nome de terceiros.

Outras classificações que os autores Damásio de Jesus e José Antônio Milagre (2016, p.61-62) descreve a figura de *White Hats, Gray Hats* e *Black Hats:*

> 1.*Black Hats* são os *crackers*, pessoas com elevados conhecimentos de tecnologia que os utilizam para atividades criminosas.
> 2.*White Hats* seriam os *hackers*, ou ainda “*Hackers*” *éticos*, especialistas que usam suas habilidades para o bem e para o fortalecimento da segurança dos sistemas. Teremos ainda os *Gray Hats*, que se encaixaria em algum lugar entre o *Black* e o *White Hat*. O melhor conceito que identificamos sobre *Gray Hat* está nos exemplos de Russo (2013, p. 4), que esclarece: “Um *hacker* de chapéu branco primeiramente pede permissões à corporação ou empresa antes de testar a segurança de *sites*, *softwares* ou sistemas. Caso descubra alguma falha em sua exploração, o mesmo alerta sigilosamente todos os envolvidos após comprometê-los. Já o *Hacker* de chapéu cinza não utiliza o seu acesso indevido para fins maléficos, mas caso ele acesse um sistema de segurança, o mesmo já está comprometido, fato que torna a ação do *Hacker Gray Hat* totalmente ilegal. Se um *hacker* de chapéu cinza descobre uma falha de segurança em um *software* ou *site*, o *Hacker Grey Hat* pode revelar esta falha publicamente para a empresa do sistema invadido, ao invés de divulgar em particular aos responsáveis como o *White Hat* faria. Deste modo eles não iriam se aproveitar da falha de segurança para seu próprio benefício”.

2.4 SUJEITO PASSIVO

O sujeito passivo da ação é aquele que de fato sofreu com a conduta criminosa, cuida-se de crime comum, podendo ser qualquer pessoa, não há necessidade de características especiais. A vítima pode ser pessoa física ou jurídica, pública ou particular e sempre haverá um lesado nessas condutas.

A doutrina classifica o sujeito passivo em duas espécies, formal e material: Sujeito passivo formal, será sempre o Estado, pois assim como a sociedade, ele também é prejudicado quando as leis não são respeitadas e os crimes são praticados. Do outro lado o sujeito passivo material é o titular do bem jurídico ofendido, podendo ser pessoa física ou jurídica.

2.5 PRINCIPAIS TIPOS PENAIS NO CIBERESPAÇO

Os delitos mais comuns cometidos na internet já eram previstos como crimes desde muito antes da rede mundial de computadores ficar on-line. O fato desses crimes serem cometidos no meio digital é apenas uma circunstância adicional. No Brasil os crimes mais comuns na rede são:

> [...]o estelionato e a pornografia infantil. Os *emails* gratuitos são outro agente de expansão, pois seus dados não são necessariamente comprovados. Uma prática recomendável seria obrigar os provedores a identificar suas contas ativas e inativas, utilizando uma tecnologia de fotografia do usuário, ou seja, ter a comprovação de seus dados e, se possível, sua imagem digital. Isso, associado a uma prática de recadastramento dos usuários, no mesmo procedimento adotado pelos bancos, permite que realmente existem meios de prova confiáveis, rompendo-se a maior barreira à segurança na rede. (PINHEIRO, 2013, p. 122)

O Código Penal quando se refere aos crimes digitais traz dois artigos específicos que são: artigos 154-A e 298 que falam o exposto a seguir:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. [...]
>
> 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. Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito. (BRASIL, 1940)

Dentre os crimes virtuais, podemos destacar esses, cujas práticas são as mais corriqueiras, são elas:

2.5.1 Pedofilia

A pedofilia é caracterizada como uma doença, um desvio de sexualidade, que leva um indivíduo adulto a se sentir sexualmente atraído por crianças e adolescentes de forma compulsiva e obsessiva, podendo levar ao abuso sexual. O pedófilo é, na maioria das vezes, uma pessoa que aparenta normalidade no meio profissional e na

sociedade. Ele se torna criminoso quando utiliza o corpo de uma criança ou adolescente para sua satisfação sexual, com ou sem o uso da violência física[2].

O DSM. IV – Manual de Diagnóstico e Estatística da Associação Norte-Americana de Psiquiatria, define a pedofilia da seguinte forma:

> O foco parafílico da pedofilia envolve atividade sexual com uma criança pré-púbere (geralmente com 13 anos ou menos). O indivíduo com pedofilia deve ter 16 anos ou mais e ser pelo menos 5 anos mais velho que a criança. Para indivíduos com pedofilia no final da adolescência, não se específica uma diferença etária precisa, cabendo exercer o julgamento clínico, pois é preciso levar em conta tanto a maturidade sexual da criança quanto a diferença de idade. Os indivíduos com pedofilia geralmente relatam uma atração por crianças de uma determinada faixa etária. Alguns preferem meninos, outros sentem maior atração por meninas, e outros são excitados tanto por meninos quanto por meninas.

O crime de pedofilia é cometido com muita frequência na internet, haja vista que a internet é para todos, tantos os bons usuários quando os maus, também menores e maiores de idades, ficando expostos as crianças e adolescentes partes mais vulneráveis.

A legislação penal acerca dos crimes contra a dignidade sexual, possui capítulo específico nomeado dos crimes sexuais contra vulneráveis em que estão previstos os artigos 217-A (estupro de vulnerável); Artigo 218 prevê a mediação de menor de 14 anos para satisfazer a lascívia de outrem; art. 218-A– satisfação da lascívia mediante a presença de menor de 14 anos; 218-B – favorecimento da prostituição ou outra forma de exploração sexual de criança, adolescente ou vulnerável.

Por sua vez a legislação especial prevê no Estatuto da Criança de do Adolescente crimes envolvendo a pedofilia nos artigos 240 utilização de criança ou adolescente em cena de sexo explícito ou pornográfica; art. 241 comércio de material pedófilo; art. 241-A difusão de pedofilia; art. 241-B posse de material pedófilo; art. 241-C simulacro de pedofilia; art. 241-D aliciamento de crianças.

Após o Estatuto da Criança e do Adolescente entrar em vigor, a lei trouxe dispositivos legais que tratou sobre o crime de pornografia infantil, porém os artigos vieram repleto de lacunas. Anteriormente, pela leitura da redação original do artigo

---

[2] MPDFT, o que é pedofilia? Disponível em https://www.mpdft.mp.br/portal/index.php/conhecampdft-menu/nucleos-e-grupos/nevesca/perguntas-frequentes-mainmenu-428/3194-o-que-e-pedofilia Acesso em 09 de out 2020

241[3] entendia-se a conduta de “fotografar ou publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente" como criminosa. Nesses termos várias condutas não se enquadrariam como pornografia, a exemplo o envio de um e-mail com pornografia envolvendo criança ou adolescente. Após duras críticas, o ECA foi reformulado[4] e hoje abarca esta possibilidade e outras semelhantes.

A legislação Brasileira adaptou-se para englobar os crimes cibernéticos cometidos atualmente.

2.5.2 Estelionato

O crime de estelionato, é conceituado como a obtenção de vantagem ilícita recebida, através de artifício fraudulento que ofereça algum prejuízo à vítima. Leia-se o artigo 171 em seu inteiro teor: “Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento”.

---

[3] Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena - reclusão, de 4 (quatro) a 8 (oito) anos, e multa.

[4] Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
Pena - reclusão, de 3 (três) a 6 (seis) anos, e multa.
§ 1o Nas mesmas penas incorre quem:
I - Assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
ll - assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
§ 2o As condutas tipificadas nos incisos I e ll do § 1o deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo.
Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
Pena - reclusão, de 1 (um) a 4 (quatro) anos, e multa.
§ 1o A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo.
§ 2o Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241 A e 241-C desta Lei, quando a comunicação for feita por:
I-agente público no exercício de suas funções;
ll - membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo;
lll - representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário.

Por meio do trecho “qualquer outro meio fraudulento” surge a possibilidade de o estelionatário praticar o crime com a utilização do computador, bastando a sua utilização como meio, é o entendimento atual dos tribunais superiores.

Comete o crime de estelionato o agente que introduz um dispositivo conhecido como “chupa-cabra” em um caixa eletrônico para conseguir o número e a senha de um cartão. Da mesma forma comete estelionato virtual quem insere cartão adulterado no caixa eletrônico, que a máquina interpreta ser legítimo, porém as informações transmitidas são fraudulentas.

Outra forma de se propagar o crime é aquele agente que cria página na internet ou faz anúncios em sites de vendas coletivas como o mercado livre, olx, entre outros, com objetivo de simular venda de algum produto, induzido a vítima ao erro de efetuar o pagamento antecipado, para receber a mercadoria posteriormente, sendo que se trata de um golpe onde o agente se aproveita da boa-fé dos outros para obter para si ou outrem vantagem econômica indevida.

Sobre o tema importante destacar o projeto de lei 3376/2020 que pretende inserir a modalidade de estelionato virtual no Código Penal. Pela leitura do texto em tramitação na Câmara dos Deputados, essa modalidade terá pena de reclusão, de 2 a 10 anos, e multa – o dobro daquela prevista para o estelionato.

2.5.3 Ameaça

O crime de ameaça está previsto no artigo 147 do Código Penal, *in verbis*: Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave: Pena - detenção, de um a seis meses, ou multa. Parágrafo único - Somente se procede mediante representação (BRASIL, 1940).

A ameaça é um crime de menor potencial ofensivo, por isso é processado e julgado nos juizados especiais criminais, a pena do condenado pode ser substituída por penas alternativas como a prestação de serviço à comunidade, ou pagamento de cestas básicas a alguma instituição.

No mundo virtual, a ameaça ganha os mesmos termos, com poucas diferenças, para ocorrer o crime o criminoso precisa oferecer algum temor para a vítima. O crime se consome a partir do conhecimento da ameaça pela vítima.

2.5.4. Dos crimes contra a honra

A honra pode ser entendida como o conjunto de atributos morais, intelectuais e físicos que se referem a uma pessoa.

> “Independe de qualquer que seja a definição dada a honra, ela é um interesse penalmente protegido. É importante, do ponto de vista de o amparo penal à honra, pois “ela não diz respeito apenas ao interesse exclusivo do indivíduo, mas também da coletividade, que tem interesse na preservação da honra, da incolumidade moral e da intimidade além de outros bens jurídicos indispensáveis para a harmonia social. ” (BITTENCOURT, 2011, p.314)

O crime de calúnia está previsto no artigo 138[5] do Código Penal, é a pratica de imputar a outrem fato criminoso, ferindo a honra da vítima. É crime comum, todos podem cometer, também é punível contra a honra dos mortos.

A acusação caluniosa não precisa ser feita diante do ofendido, basta as ofensas se tornar públicas, devendo haver a intenção de divulgar fato criminoso sabendo ser falso.

O crime é praticado em qualquer meio de execução, portanto pode ser através do uso palavra, por escrito, ou em outros meios, todavia, as ofensas devem chegar ao conhecimento de outras pessoas que não o ofendido, para a consumação do crime.

O exemplo disso no meio virtual são os xingamentos nas redes sociais imputando fatos criminosos que o agente sabe se tratar de uma mentira.

A difamação por sua vez está prevista no artigo 139[6] do Código Penal, para que se caracterize a calúnia, precisa haver uma falsa imputação de fato definido como crime de forma determinada e específica, em que a outra pessoa toma conhecimento,

---

[5] Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime:
Pena - detenção, de seis meses a dois anos, e multa.
§ 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.
§ 2º - É punível a calúnia contra os mortos. Exceção da verdade
§ 3º - Admite-se a prova da verdade, salvo:
I - se, constituindo o fato imputado crime de ação privada, o ofendido não foi condenado por sentença irrecorrível;
II - se o fato é imputado a qualquer das pessoas indicadas no nº I do art. 141;
III - se do crime imputado, embora de ação pública, o ofendido foi absolvido por sentença irrecorrível.

[6] Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
Pena - detenção, de três meses a um ano, e multa.
Exceção da verdade
Parágrafo único - A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções.

não necessariamente a vítima. Diferente da calúnia, a imputação não precisa ser falsa, basta o fato desabonar a honra da vítima.

Na internet, a difamação ocorre sempre quando alguém ofende a dignidade da outra, isso ocorre frequentemente nas redes sociais quando alguém faz uma acusação de um fato criminoso a outrem.

Por fim a injúria é o ato que ofende a dignidade da pessoa. Significa atribuir a outrem adjetivo negativo que pode ser falso ou verdadeiro. Nesse caso não há a imputação de um fato, mas sim o agente profere uma opinião negativa (xingamento) a respeito da vítima, ofendendo a sua honra subjetiva.

Segundo Fernando Capez: “Ao contrário da calúnia e a difamação que tutelam a honra objetiva, por essa norma penal é a honra subjetiva, que é constituída pelo sentimento próprio de cada pessoa acerca de seus atributos morais, intelectuais e físicos. (2018, p.252)

A injúria é cometida tanto de forma verbal, escrita, quanto física, essa última é mais grave e possui a pena agravada. Na internet os crimes de ódio ocorrem diariamente, pessoas se escondem atrás de uma tela para xingar e ofender as vítimas, caso ocorra a ofensa e tenha elemento extraído de raça, cor, etnia, o crime cometido é o de injúria racial, conduta mais gravosa com pena de reclusão de um a três anos e multa, conforme a Lei 9.459/97. Ademais a vítima poderá pleitear reparação civil pelo dano sofrido à sua honra.

3 LEGISLAÇÃO ATUAL, COMPETÊNCIA E INVESTIGAÇÃO

A legislação vigente, uma boa base na investigação e a perícia são mecanismos de combate aos crimes virtuais no Direito Penal e são essenciais para a condução da instrução probatória e na resolução nos processos criminais, consequentemente o agente criminoso, que se utiliza do meio virtual para violar bem jurídicos tutelados pela norma penal, é punido. A sensação que os mecanismos trazer é de repressão as condutas maliciosas na internet e a provável inibição do seu crescimento.

3.1 LEGISLAÇÃO VIGENTE

O artigo art. 5º, XXXIX da Constituição Federal consagra o princípio da reserva legal e da legalidade e assim prevê que: “Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal”. Dessa forma, as condutas não tipificadas em lei e aquelas formuladas sem a observância ao devido processo legislativo, não podem ser considerados crimes.

Para Marco Antônio Marques da Silva, o princípio da legalidade ou reserva legal é um limitador do poder punitivo e normativo do Estado, pois há um empecilho na criação de tipos penais, exceto o regular processo legislativo. O autor prossegue dizendo que referido princípio é uma “consequência direta do fundamento da dignidade da pessoa humana, pois remonta à ideia de proteção e desenvolvimento da pessoa que o tem como referencial” (SILVA, 2001, p.07).

De acordo com a Constituição Federal Brasileira o Código Penal Brasileiro prevê no artigo primeiro que “Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal”.

No Brasil, até o ano de 2012 não existia no ordenamento brasileiro legislação especifica para a tipificação dos crimes informáticos. As normas já existentes eram utilizadas pelos operadores de direito para preencher as lacunas na lei. Com o avanço da tecnologia e o uso malicioso dessa plataforma era cada vez mais necessária instituir uma legislação específica que enquadrasse esses delitos. Nas palavras de MASSON:

> É inegável que leis editadas décadas atrás, nas quais sequer se pensava na existência de computadores, levavam a malabarismos adaptativos dos operadores do Direito para enfrentar novos comportamentos, muitas vezes resultando na impunidade dos criminosos. Era preciso adaptar a legislação penal aos novos tempos. (2016, p. 276)

No ordenamento pátrio existia somente a lei nº 9.296/96 que regulamentava o art. 5º, XII, da Constituição Federal, o qual assegura a inviolabilidade das comunicações. A lei, em seu artigo 10 deu um grande passo ao estabelecer pena de até 4 anos de reclusão, e multa, no caso de o indivíduo “realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei”.

Depois de aproximadamente uma década de discussões e trâmite no Congresso Nacional, através do projeto encabeçado pelo Deputado Federal Luiz Piauhylino*,* autor do PL nº 84/99, foi aprovada a lei *12.737/2012,* popularmente conhecida como Lei Carolina Dieckmann. Também foi sancionada a Lei 12.735, que trata da necessidade de instalação de órgãos investigativos especializados.

O percurso até a criação da lei ocorreu após intensos debates a respeito da criação de leis que tipificassem crimes cometidos na internet, também teve um impulso após o caso da atriz Carolina Dieckmann, situação na qual criminosos invadiram sua conta pessoal eletrônica e divulgaram inúmeras fotos íntimas da atriz, na época pela falta de base legal os agentes foram responsabilizados pelos crimes de extorsão, difamação e furto, todavia a conduta de invadir o computador não pode ser enquadrada.

Conforme NUCCI *apud* SANCHES (2016), ressalta a importância da criação da lei supramencionada que tipificou a conduta:

> Sabe-se, por certo, constituir a comunicação telemática o atual meio mais difundido de transmissão de mensagens de roda a ordem entre pessoas físicas e jurídicas. O e-mail tornou-se uma forma padrão de enviar informes e mensagens profissionais e particulares, seja para fins comerciais, seja para outras finalidades das mais diversas possíveis. *As* redes sociais criaram, também, mecanismos de comunicação, com dispositivos próprios de transmissão de mensagens. Torna-se cada vez mais rara a utilização de cartas e outras bases físicas, suportando escritos, para a comunicação de dados e informes. Diante disso, criou-se novel figura típica incriminadora, buscando punir quem viole não apenas a comunicação telemática, mas também *os* dispositivos informáticos, que mantém dados relevantes do seu proprietário. (p. 774-775)

A lei 12.737, incluiu no Código Penal Brasileiro o tipo penal invasão de dispositivo informático no Art. 154-A e instituiu a regra da ação penal para esse crime Art. 154-B, in verbis:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: (Incluído pela Lei nº 12.737, de 2012) Vigência
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. (Incluído pela Lei nº 12.737, de 2012) Vigência
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. (Incluído pela Lei nº 12.737, de 2012) Vigência
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico. (Incluído pela Lei nº 12.737, de 2012) Vigência
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações

> sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: (Incluído pela Lei nº 12.737, de 2012) Vigência
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. (Incluído pela Lei nº 12.737, de 2012) Vigência
> § 4º Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos. (Incluído pela Lei nº 12.737, de 2012) Vigência
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra: (Incluído pela Lei nº 12.737, de 2012) Vigência
> I - Presidente da República, governadores e prefeitos; (Incluído pela Lei nº 12.737, de 2012) Vigência
> II - Presidente do Supremo Tribunal Federal; (Incluído pela Lei nº 12.737, de 2012) Vigência
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou (Incluído pela Lei nº 12.737, de 2012) Vigência
> IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (Incluído pela Lei nº 12.737, de 2012) Vigência
> **Ação penal** (Incluído pela Lei nº 12.737, de 2012) Vigência
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos. (Incluído pela Lei nº 12.737, de 2012) Vigência (BRASIL.2012)

Ademais também alterou a redação dos artigos 266[7] e 298[8] do Código Penal, de modo que passou a punir condutas como a de uso não autorizado de dados de cartões de crédito e débito obtidos de forma indevida, invasão de dispositivos eletrônicos alheios conectados ou não à internet, produção, oferta e venda de programas de computadores que permitam a invasão com vírus de internet e obtenção

---

[7] 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.
~~Parágrafo único - Aplicam-se as penas em dobro, se o crime é cometido por ocasião de calamidade pública.~~
§ 1 º 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
§ 2 º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública. (Incluído pela Lei nº 12.737, de 2012) Vigência

[8] 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

de informações sigilosas ou violação de comunicações eletrônicas privadas ou segredos comerciais.

Patrícia Peck Pinheiro faz uma breve análise sobre as mudanças da lei 12.737/2012 e aduz que:

> “Ainda, receberá as mesmas penas da invasão aquele que instala uma vulnerabilidade em um sistema de informação para obter vantagem indevida, por exemplo, um *backdoor* ou uma configuração para que algumas portas de comunicação à internet fiquem sempre abertas. 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. ” (2013, p. 207)

3.1.1 Marco Civil da Internet (Lei 12.965/2014)

A denominada Lei 12.965/2014, conhecida como o Marco Civil da Internet dispõe sobre os direitos e deveres dos usuários da internet. Estabelece princípios, garantias e obrigações para o uso da Internet no Brasil. A lei protege os dados pessoais e a privacidade dos usuários. Sendo assim, uma possível quebra de dados e informações particulares só é possível mediante ordem judicial.

PINHEIRO explica que “Legislar sobre a matéria de crimes na era Digital é extremamente difícil e delicado. Isso porque sem a devida redação do novo tipo penal corre-se o risco de se acabar punindo o inocente”. (2016, p. 259)

Buscando elucidar questões como princípios, garantia da proteção dos dados pessoais e privacidade dos usuários, direitos e deveres para quem utiliza a internet, bem como traçar diretrizes para a atuação do Estado, foi criado a Lei nº 12.965/147.

O Marco Civil da Internet no Brasil cumpriu um papel fundamental para a legislação brasileira, pois trouxe um grande amadurecimento sobre questões que eram de grande desafio para o judiciário. Trazendo soluções adequadas para a nova realidade enfrentada nos casos concertos.

3.2 DA COMPETÊNCIA PARA PROCESSAR E JULGAR

A jurisdição consiste na atuação do Estado para aplicação do Direito vigente a um determinado caso concreto, cujo objetivo é resolver de forma decisiva e sanar todo o imbróglio jurídico e por fim conferir a paz social.

Por sua vez, a competência, pode ser entendida como a medida da Jurisdição, ou, para alguns doutrinadores, o limite da Jurisdição. Em outras palavras, a Competência é o conjunto de regras que estabelecem os limites em que cada Juiz pode exercer, de maneira válida, o seu Poder Jurisdicional. (NUCCI, 2015, p. 205)

A aplicação da lei Processual Penal no espaço rege-se pelo princípio da territorialidade que é conceituado com a aplicação da lei processual penal brasileira em todo crime ocorrido em território nacional[9], em consonância com a norma penal no artigo. 5.º: Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional. (BRASIL, 1940)

> É regra que assegura a soberania nacional, tendo em vista não haver sentido aplicar normas procedimentais estrangeiras para apurar e punir um delito ocorrido dentro do território brasileiro. O direito alienígena é composto pela vontade de outro povo, razão pela qual os magistrados, em nosso país, não cumprem e não devem, de fato, seguir legislação que não seja fruto do exclusivo desejo da nação brasileira. (NUCCI, Guilherme de Souza, 2020, p.287)

Nestor Távora explica que: “Conforme o entendimento de TÁVORA “a competência passa a ser um critério legal de administração eficiente da atividade dos órgãos jurisdicionais, definindo previamente a margem de atuação de cada um, isto é, externando os limites de poder” (2017, p. 387).

Ademais sobre os fatores que afastam a competência de determinado juízo podem ser, nas palavras do doutrinador Guilherme de Souza Nucci:

> Um dos fatores de afastamento da aplicação da lei processual penal é a ressalva feita aos tratados, convenções e regras de direito internacional (art. 1.º, I, CPP). Além disso, prevê o art. 5.º, § 4.º, da Constituição Federal (Emenda Constitucional 45/2004) que “o Brasil se submete à jurisdição de Tribunal Penal Internacional a cuja criação tenha manifestado adesão”.

---

[9]Art. 1º O processo penal reger-se-á, em todo o território brasileiro, por este Código, ressalvados:
I - os tratados, as convenções e regras de direito internacional;
II - as prerrogativas constitucionais do Presidente da República, dos ministros de Estado, nos crimes conexos com os do Presidente da República, e dos ministros do Supremo Tribunal Federal, nos crimes de responsabilidade (Constituição, arts. 86, 89, § 2º, e 100);
III - os processos da competência da Justiça Militar;
IV - os processos da competência do tribunal especial (Constituição, art. 122, nº 17);
V - os processos por crimes de imprensa. (Vide ADPF nº 130)

> Significa, pois, que, apesar de um delito ser cometido no país, havendo interesse do Tribunal Penal, podemos entregar o agente à jurisdição estrangeira (exceto quando se tratar de brasileiro, pois o próprio art. 5.º,LI, a veda, constituindo norma específica em relação ao § 4.º). (2020, p.287,288)

A Competência material pode ser definida em: Competência em razão da matéria (ratione materiae) –prevista no inciso I do artigo citado, é definida com base no fato a ser julgado; Competência em razão da pessoa (ratione personae) – leva em conta as condições relativas às pessoas que se encontram como rés no processo criminal (polo passivo/os acusados); e Competência territorial (ratione loci) – Considera o local onde ocorreu a para que seja definida a competência, ou leva em conta outros critérios territoriais.

O artigo 69 do Código de Processo Penal, traz sete critérios para a fixação da competência: **I - o lugar da infração: II - o domicílio ou residência do réu; III - a natureza da infração**; IV - a distribuição; V - a conexão ou continência; VI - a prevenção; **VII - a prerrogativa de função**.

Na doutrina somente os itens I, II, III, e VII são considerados como critérios de fixação de competência criminal. Os outros incisos são parâmetros para consolidação da competência após a ocorrência do fato a ser julgado, em razão da existência de mais de um órgão jurisdicional previamente competente para julgar o caso.

A Competência em razão da matéria (ratione materiae) ou competência de jurisdição ou justiça leva em consideração a natureza do fato criminoso para definir qual a será a justiça competente. Dessa forma a competência criminal em razão da matéria é dividida basicamente em: Comum e especial. A Justiça comum se divide em Federal e Estadual. A Justiça Especial por sua vez se divide em Eleitoral e Militar.

A Justiça Especial Eleitoral e Militar julga somente os crimes da sua alçada. A justiça estadual é residual, ou seja, todos os outros crimes que não sejam da competência da justiça comum federal ou especializada são de competência da Justiça Comum.

Quanto os critérios para a fixação da justiça federal o domínio da matéria é mais restrito, pois só há declínio de competência da justiça estadual para federal quando envolver grave violação dos direitos humanos, de previsão constitucional e em face de tratados e convenções em que o Brasil é signatário. É o que diz as hipóteses do artigo 109 da CF/88:

> Art. 109. Aos juízes federais compete processar e julgar: (...) IV - os crimes políticos e as infrações penais praticadas em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas,

> excluídas as contravenções e ressalvada a competência da Justiça Militar e da Justiça Eleitoral; V - os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente; V-A as causas relativas a direitos humanos a que se refere o § 5º deste artigo;(Incluído pela Emenda Constitucional nº 45, de 2004) VI - os crimes contra a organização do trabalho e, nos casos determinados por lei, contra o sistema financeiro e a ordem econômico-financeira; VII - os "habeas-corpus", em matéria criminal de sua competência ou quando o constrangimento provier de autoridade cujos atos não estejam diretamente sujeitos a outra jurisdição; VIII - os mandados de segurança e os "habeas-data" contra ato de autoridade federal, excetuados os casos de competência dos tribunais federais; IX - os crimes cometidos a bordo de navios ou aeronaves, ressalvada a competência da Justiça Militar; X - os crimes de ingresso ou permanência irregular de estrangeiro, a execução de carta rogatória, após o "exequatur", e de sentença estrangeira, após a homologação, as causas referentes à nacionalidade, inclusive a respectiva opção, e à naturalização; XI - a disputa sobre direitos indígenas. (...) § 5º Nas hipóteses de grave violação de direitos humanos, o Procurador-Geral da República, com a finalidade de assegurar o cumprimento de obrigações decorrentes de tratados internacionais de direitos humanos dos quais o Brasil seja parte, poderá suscitar, perante o Superior Tribunal de Justiça, em qualquer fase do inquérito ou processo, incidente de deslocamento de competência para a Justiça Federal. (Incluído pela Emenda Constitucional nº 45, de 2004)

Todas as matérias que não se enquadrem na competência da Justiça Comum Federal, serão de competência da Justiça Comum Estadual.

O Código de Processo Penal trata de uma hipótese de competência em razão da natureza da infração: A competência do Tribunal do Júri.

A Competência em razão da pessoa (ratione personae) evidencia a regra do Código de Processo Penal, em que os processos criminais são julgados pelos Juízes de primeiro grau. Todavia, pode acontecer em determinados casos, considerando a presença de determinadas autoridades no polo passivo, que a competência seja originariamente aos Tribunais. Dá-se o nome de prerrogativa de função, também conhecida por “foro privilegiado”.

Por fim, a competência territorial (*ratione loci*) compreende a análise do local de ocorrência da infração ou do domicílio do réu que irá determinar em que base territorial será o processo julgado, qual comarca, se será na Justiça Estadual, ou Seção Judiciária, quando for da competência da Justiça Federal.

Os artigos 69, inciso I, 70 e 71, ambos do Código de Processo Penal, elucidam os critérios para adotar a competência em razão do local da infração, entendido pelo juízo territorialmente competente. In verbis:

> Art. 69. Determinará a competência jurisdicional:
> I - O lugar da infração:
> Artigo 70. A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução. ”

> Art. 71**.** Tratando-se de infração continuada ou permanente, praticada em território de duas ou mais jurisdições, a competência firmar-se-á pela prevenção (BRASIL, 1941)

O local do crime no direito penal é definido pela Teoria da Ubiquidade, a qual explica que o local do crime é aquele no qual o agente consumou o fato ou cessou o último ato executório do delito. De acordo com o artigo 6º do Código Penal, in verbis: “Artigo 6º. Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado.”

> Desta feita, para que se possa identificar qual o juízo competente para o processo e julgamento de cada crime, faz-se necessário a análise dessas 3 espécies de competência principalmente, começando pelo local onde se consumou a infração ou foi praticado o último ato de ação ou omissão, para se determinar qual o local competente para o julgamento do feito, seguindo com a natureza do delito para que possa se distribuir o processo para a vara competente e, importante também analisar se o réu tem prerrogativa de função ou não, para saber se o processo correrá em sede de 1º grau de jurisdição ou em tribunais superiores, não necessariamente nessa ordem. (SOUZA, Competência para processar e julgar crimes virtuais. Disponível em:<https://lucasaps91.jusbrasil.com.br/artigos/417311418/competencia-para-processar-e-julgar-crimes-virtuais/> Acesso em 10 de nov. de 2020.

Tecidos os conceitos de espécies de competência prosseguimos para as grandes questões sobre a competência para processar e julgar os crimes virtuais

Embora o Código de Processo Penal confira alguns critérios para a fixação e consolidação da competência, o presente trabalho para fins didáticos e elucidativo irá se ater apenas a Competência em razão da matéria (ratione materiae) ou competência de Jurisdição ou competência de Justiça.

A conexão da Internet cria uma teia global, cobrindo e interligando diversos dispositivos eletrônicos pelo mundo a fora. O ordenamento jurídico de cada Estado é determinado de forma autônoma, respeitando a Soberania de um país.

A jurisdição e a competência para processar e julgar os crimes virtuais são apuradas sucintamente no âmbito do Processo Penal posto que há uma preocupação para aplicar a lei corretamente ao caso concreto. A necessidade de se definir a competência ocorre porque o ambiente virtual não é mensurável, ele se interliga e interage com diversos países, e conecta inúmeros indivíduos, abrange todo o território virtual, não há como delimitar fronteiras físicas.

Na legislação atual no tocante a aplicação da lei aos delitos virtuais não existe tratamento universal, também em relação aos tratados de direito sobre o tema, muitas vezes, não são todos os países signatários, ou não há reciprocidade por vezes, dessa

forma a investigação e a punibilidade desses atos são dificultadas. Marco Aurélio Greco afirma que: “Além das repercussões na ideia de soberania e na eficácia das legislações, não se pode deixar de mencionar os reflexos que serão gerados em relação ao exercício da função jurisdicional” (2000, p.15)

Para se apurar a competência na prática legal dos crimes cibernéticos existem alguns desafios que são observados posto que há inúmeros tipos penais que diferem as formas de consumação e o resultado do crime.

De acordo com a jurisprudência do Superior Tribunal de Justiça, somente pelo fato de um crime ter sido cometido pela internet por si só não atrai a competência da justiça federal para processar e julgar o crime. É necessário demonstrar a internacionalidade da conduta ou de seus resultados.

> PENAL E PROCESSUAL PENAL. CONFLITO NEGATIVO DE COMPETÊNCIA. COMPARTILHAMENTO DE SINAL DE TV POR ASSINATURA, VIA SATÉLITE OU CABO. CARD SHARING. ARTIGO 109, INCISO V, DA CF/88. NORMATIVO INTERNACIONAL VIGENTE. TRANSNACIONALIDADE DA CONDUTA. COMPETÊNCIA DA JUSTIÇA FEDERAL.
> 1. De acordo com o art. 109, V, da Constituição Federal, a competência da jurisdição federal se dá pela presença concomitante da transnacionalidade do delito e da assunção de compromisso internacional de repressão, constante de tratados ou convenções internacionais. 2. No caso em análise, o Ministério Público do Estado de São Paulo, a partir de notitia criminis formulada pela Associação Brasileira de Televisão por Assinatura, requereu a busca e apreensão de elementos de prova acerca da prática de crimes de violação de direitos autorais e contra a Lei de Software, relacionados à atividade de fornecimento ilícito de sinal de TV por assinatura.
> 3. O requisito inicial de previsão normativa internacional é constatado pela Convenção de Berna, integrada ao ordenamento jurídico nacional através do Decreto nº 75.699, de 6 de maio de 1975, e reiterada na Organização Mundial do Comércio - OMC por acordos como o TRIPS (Trade-Related Aspects of Intellectual Property Rights) - Acordo sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados ao Comércio (AADPIC), incorporado pelo Decreto nº 1355, de 30 de Dezembro de 1994, com a previsão dos princípios de proteção ao direitos dos criadores, além de diversos outros tratados e convenções multilaterais assinados pelo Brasil, fixando garantias aos patrimônios autorais e culturais.
> 4. O segundo requisito constitucional, de tratar-se de crime à distância, com parcela do crime no Brasil e outra parcela do iter criminis fora do país, é constatado pela inicial prova da atuação transnacional dos agentes, por meio da internet.
> 5. Conflito conhecido para declarar competente o JUÍZO FEDERAL DA 9ª VARA CRIMINAL DA SEÇÃO JUDICIÁRIA DO ESTADO DE SÃO PAULO, ora suscitante.
> (CC 150.629/SP, Rel. Ministro NEFI CORDEIRO, TERCEIRA SEÇÃO, julgado em 22/02/2018, DJe 28/02/2018)

A competência dos crimes virtuais só será da Justiça Federal quando o crime produzir seus efeitos no exterior e o Brasil for signatário de tratado ou convenção internacional que tenha dispositivo legal que aceite a atuação do ordenamento jurídico

brasileiro no combate do crime correlato. Essas são as hipóteses, não se enquadrando em nenhuma delas a justiça comum estadual terá a competência para processar e julgar os crimes virtuais.

> “Conforme a situação concreta, o delito pode consumar-se no momento em que a informação é veiculada na rede mundial e pode ser acessada a qualquer momento por qualquer usuário, como também pode ter a sua consumação postergada. Exemplo deste último caso, seria a prática de estelionato, em que o autor prepara a fraude, invade algum site, implanta um software, que somente produzirá efeito posterior, subtraindo ou desviando bens ou valores de alguém. Não se tratando de delito previsto em tratado internacional, ou de caráter transnacional, a competência é da Justiça Estadual. Porém, quando a conduta do agente implicar, automaticamente, em acesso imediato por outros usuários, pode-se considerar que a consumação é dúplice, vale dizer, dá-se em território nacional e, concomitantemente, em outros países. Assim ocorrendo, se a infração penal tiver previsão em tratado ou convenção subscrita pelo Brasil, a competência é federal. ” NUCCI, 2016, p. 178.

3.3 INVESTIGAÇÃO DE CRIMES CIBERNÉTICOS

No presente tópico serão apresentadas as questões relacionadas a investigação criminal dos crimes cibernéticos quanto a prova no processo penal. Primeiramente, será discutida a dificuldade na identificação de autoria e da prova da materialidade.

A Investigação criminal compõe um conjunto de diligências iniciais devidamente formalizadas que, dentro da lei, buscam apurar a existência, materialidade, circunstâncias e autoria de uma infração penal.

No ordenamento jurídico brasileiro, não existe impedimento na utilização de provas eletrônicas, conforme versa o art. 225 do Código Civil:

> 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)

O art. 369 do Código De Processo Civil de 2015 também possibilita todos os meios legais de prova e prevê:

> As partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz. (BRASIL, 2015)

Ademais, o Código de processo penal também aceita as provas eletrônicas, conforme versa o art. 231, “salvo os casos expressos em lei, as partes poderão apresentar documentos em qualquer fase do processo”, corroborando com o artigo retro, o art. 232 também versa que “consideram-se documentos quaisquer escritos, instrumentos ou papéis, públicos ou particulares”.

Quando um usuário utiliza a rede mundial de computadores, mediante um dispositivo eletrônico, recebe uma identificação virtual denominado de *internet Protocol* conhecido como endereço de IP. É um número identificador conferido ao computador ou roteador.

O IP é principal protocolo de comunicação da internet, também responsável por enviar e receber dados na internet. O número identificador é disponibilizado ao usuário através de um provedor de acesso, onde consta no sistema a hora, data e fuso horário do local. São elementos fundamentais para a verificação de sigilo de dados.

É por intermédio do provedor de acesso à internet que após decisão judicial deferindo a quebra de sigilo de dados informáticos, que é possível vincular o endereço de IP distribuído ao usuário naquela data e hora em que ocorreu o crime, ao seu endereço físico.

Burg, advogado especialista em crimes virtuais, elenca as dificuldades de investigação dos crimes referidos:

> A internet facilita a impunidade, uma vez que a investigação é mais complicada e, muitas vezes, quando é identificado o autor, já ocorreu a prescrição. Isso sem contar na questão da fronteira: o crime pode ser cometido por alguém que está em outro país, com leis completamente diferentes. A fronteira acaba motivando também, de certa forma, a impunidade. E aqui, infelizmente, não tem muito o que fazer. Porque não tem como criar uma lei obrigando o cidadão da Estônia a vir para o Brasil no prazo. [...]A legislação brasileira não está adequada e, muitas vezes, o crime prescreve sem que haja um avanço significativo nas investigações. Nos crimes contra a honra, por exemplo, há uma enorme dificuldade para se identificar o autor de ofensas realizadas na internet, e sem a identificação sequer é possível oferecer queixa-crime.(Disponível em https://www.conjur.com.br/2017-fev-05/entrevista-daniel-burg especialistacrimes virtuais, acesso em 07 de nov. 2020)

3.3.1 Problemática da Prova da Autoria e Materialidade nos Crimes Cibernéticos

No espaço virtual a ausência física do agente delituoso compromete em muito a obtenção de indícios de autoria do delito, posto que o anonimato é característica precípua do uso da internet. Esse anonimato na sede é relativo, tendo em vista que no direito digital a forma de identificação virtual se dá através do endereço de IP (protocolo de internet).

Muitas identidades virtuais podem não ter correspondência com a realidade real, a identidade do agente pode não ser a mesma em que se apresenta na rede. De forma análoga é o mesmo que ocorre com as famosas “laranjas”, pessoas físicas ou jurídicas (empresas) que cedem seus dados para fins ilícitos, por exemplo como ocorre com contas e empresas fantasmas, nas quais a identidade física pode ser falsa. Assim sendo, na rede globalizada a dimensão e a facilitação para a criação de “ laranjas” tornam os riscos maiores.

Para se chegar a prova da autoria do crime, no processo penal a prova judiciária compreende na reconstrução da verdade dos fatos, ou seja, busca-se o elo existente no campo dos fatos investigados e a realidade no tempo e espaço do crime.

Todo o instrumento probatório recolhido durante a persecução penal é utilizado para o convencimento do juiz a respeito da existência dos fatos. A condenação deve ser embasada de acordo com todo o conjunto provatório que deve ser sólido, não dando margem para dúvidas e suposições. Para que o autor do crime cibernético seja punido e tenha pena aplicada, é necessária que a comprovação não tenha sido baseada em simples inferência sobre a autoria do delito, deve haver comprovação de que aquele autor de fato cometeu o crime.

Especialmente no tocante aos crimes cibernéticos, a correta identificação do suspeito gera preocupação para que a pretensão punitiva seja justa e direcionada para àquele que realmente cometeu o crime. O zelo é ainda mais pela facilidade que os agentes criminosos têm de apropriaram-se de dados, senhas e códigos de acesso de outrem e dessa forma utilizarem para aplicar golpes atrás dessa identidade.

O anonimato na internet fornece uma ampla liberdade que não ocorre o mesmo no mundo real. Em sua tese (DIAS, 2014) aduz que:

> Uma das características das condutas ilícitas praticadas na internet é o anonimato on-line, uma vez que o ambiente virtual em que estes crimes são praticados são caracterizados pela ausência de espaço físico. Os criminosos que acessam a rede mundial de computadores se utilizam de técnicas para ocultar sua verdadeira identidade e conduta, podendo, assim, assumir qualquer identidade que não a sua. (p.37)

Como já dito para possibilitar a identificação do computador, tablet, ou outro meio eletrônico o anonimato on-line é relativo, haja vista o computador pode ser identificado pelo número de endereço IP quando da conexão estabelecida com a rede mundial de computadores.

Ademais a rede mundial permite se aferir todo o tráfego e acessos à rede que o usuário utilizou durante um determinado período. Sobre a identificação no mundo real e no mundo virtual DIAS (2014) disserta que:

> A identificação de um indivíduo no “mundo real” e no “mundo virtual” é feita de modo semelhante. No “mundo real”, a identificação de uma pessoa na sociedade mescla uma espécie de concretização qualitativa, que corresponde à uma identificação visual, através do reconhecimento das principais características do indivíduo tais como feições, altura, voz; com 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. (p.39).

Toda investigação criminal deve considerar as evidências deixadas pelo criminoso cibernético por intermédio do endereço IP, os peritos especializados averiguam as provas e podem localizar o endereço de IP em qualquer parte do mundo.

Sobre os passos da investigação criminal dos crimes cibernéticos, Camila Barreto Andrade Dias diz:

> O primeiro passo na investigação dos crimes cibernéticos é identificar a origem da comunicação. Por meio de uma análise do tráfego de dados, se chegará ao endereço IP de origem e ao usuário que está vinculado a esse IP. Uma vez identificado o endereço IP, serão analisadas possíveis provas da prática do delito. Essa análise, feita por peritos especializados, é uma atividade extremamente complexa, considerando a presença de programas de computador cujo objetivo é o mascaramento da verdadeira identidade do autor, principalmente quando os computadores estão localizados em locais públicos tais como universidades, bibliotecas e cybercafés.
> Assim, a localização de uma pessoa no mundo virtual ocorre através da atribuição de um endereço IP no momento da conexão com a rede mundial de computadores. O problema em relação à autoria, é que essa identificação é sempre do computador, e nunca do sujeito (2014, p. 41)

A grande dificuldade em identificar o autor decorre da associação feita entre o proprietário do computador que o endereço de IP indica e o sujeito que se utilizou desse meio para cometer crime. Isso ocorre por exemplo nos crimes praticados em computadores compartilhados, *lan houses*, entre outros, como poderia identificar quem fez a ação.

A problemática da identificação de autoria não se situa na localização e identificação do computador onde foi originado o fato criminoso, mas sim, diz respeito à correta identificação de quem foi que utilizou a máquina com a vontade de cometer o ato ilícito ou de alguma forma contribuiu para o fim.

O órgão investigativo de um crime cibernético sempre estará diante de um dilema, encontrar uma forma de relacionar o endereço de IP com o sujeito que a utiliza.

Segundo Maciel Coli “a instauração de uma investigação baseada somente na mera presunção de suspeição decorrente da titularidade de um contrato de acesso à internet, por exemplo, estaria orientada pela responsabilização objetiva” que, no entanto, no direito penal referido instituto deve ser afastado (2010, p.203).

Assim sendo, o grande questionamento acerca do tema se encontra nas dificuldades encontradas para identificar o agente criminoso e se provar a materialidade dos fatos.

CONSIDERAÇÕES FINAIS

Os Objetivos da presente dissertação foram analisar a complexidade dos crimes cibernéticos ou virtuais e dificuldades encontradas pelos órgãos investigativo e acusador para indicar a autoria e provar a materialidade, bem como pretendeu pontuar as principais dificuldades encontradas na punição dos criminosos virtuais pelos operadores de direito durante a instrução probatória, explicar aspectos da legislação penal acerca da repressão aos crimes cibernéticos e identificar o problema na identificação do agente, quanto aos indícios de autoria e da prova de materialidade.

O enfoque principal foi pesquisar sobre os crimes cibernéticos na perspectiva do Direito Penal e Processual Penal brasileiro e também sob a ótica da legislação brasileira, em análise das particularidades que decorrem do ciberespaço, ambiente novo e atual para a ocorrência de crimes que impossibilitam uma boa investigação criminal.

Assim sendo, as atualizações legislativas ainda não são bastantes para resolver os problemas que são encontrados para resolver os crimes referidos. Considerou-se que a criminalidade no ambiente virtual não apenas foi responsabilizada pelo advento de novas condutas delituosas, por intermédio do computador e dispositivos eletrônicos, quanto também contribuiu para a violação de novos bens jurídicos que até então não eram salvaguardados pelo ordenamento jurídico como valores da tecnologia da informação, dados e sistemas.

As características que incidem dos crimes cibernéticos, e o dinamismo para a concretização de referida conduta, estão atrelados à investigação criminal. A instrução probatória é se suma importância considerar todos seus elementos. Dessa forma, surgem necessidades para se dar uma punição aos criminosos virtuais, as questões levantadas são a necessidade de peritos especializados, a dificuldade para se identificar a autoria e a importância da produção antecipada de provas, para se provar a materialidade desse tipo de crime.

Quanto à identificação de autoria, apesar da falsa percepção de facilidade ao se rastrear um computador e identificar o número de IP em que houve a realização da conduta, verificou-se uma dificuldade de se vincular o sujeito ativo do crime ao computador que foi realizada a prática delituosa. Colli apresenta possíveis soluções

para sanar a problemática como a biometria e a prisão em flagrante com o computador ativo.

Em atenção à grande capacidade de risco dos meios que servirão como prova do crime virtual, o instituto da produção prova antecipada recebe atenção ante a possibilidade de perdimento das provas.

Dessa forma, os problemas demonstrados na presente monografia acerca da materialidade e autoria dos crimes cibernéticos, decorrem de condutas que são crimes que merecem muita atenção além de depender da criação de mecanismos de segurança que sejam capazes de identificar o autor, coibir a conduta e inibir a ação dos criminosos virtuais, aplicando penas que sejam capazes de punir de forma justa para uma verdadeira reprimenda.

Tal conclusão reforça a ideia defendida por alguns autores, como Cleber Masson, Patrícia Peck Pinheiro e Maciel Colli, sobre não existir mais a necessidade da criação de mais leis, pois as vigentes se aplicam aos crimes virtuais pela interpretação, todavia a criação de uma política segura de reprimenda da conduta pelos agentes do Estado, resta totalmente necessária e válida.

REFERÊNCIAS

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Brasília, 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>. Acesso em: 24/10/2020

Brasil. Tribunal Regional Federal da 3ª Região. **Escola de Magistrados Investigação e prova nos crimes cibernéticos**. São Paulo: EMAG, 2017. 352p. (Cadernos de estudos; 1)

BRASIL. *Decreto-Lei no 3.689, de 3 de outubro de 1941.* **Código de Processo Penal**. Brasília, 1941. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em: 20 out. 2020.

BRITO, Auriney. **Direito Penal Informático**. São Paulo: Saraiva, 2013.

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

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

CONTE, Christiany Pegorari, FIORILLO, Celso Antônio Pacheco. **Crimes no Meio Ambiente Digital**. São Paulo: Saraiva, 2013

DIAS, Vera Marques. **A problemática da investigação do cibercrime**. 2012. Disponível em: <http://datavenia.pt/ficheiros/pdf/datavenia01.pdf#page=63>. Acesso em: 26 out. 2020.

FIORILLO, Celso Antônio Pacheco; CONTE, Christiany Pegorari. **Crimes no Meio Ambiente Digital**. São Paulo: Saraiva, 2013

GRECO, Marco Aurélio. **Internet e Direito**, 2. ed. São Paulo: Dialética, 2000.

LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computacional**. São Paulo: Editora Atlas, 2011.

KUNRATH, Josefa Cristina Tomaz Martins. **A expansão da criminalidade no cyberespaço**/ Josefa Cristina Tomaz Martins Kunrath. –Feira de Santana : Universidade Estadual de Feira de Santana, 2017.

MIRABETE, Julio Fabbrini; FABBRINI, Renato. **Manual de direito penal – parte geral**, v. I. 23ª ed. São Paulo: Atlas, 2006.

NUCCI, Guilherme de Souza. **Código de Processo Penal Comentado**, 15ª ed. Rio de Janeiro: Forense, 2016.

NUCCI, Guilherme de Souza. **Curso de direito processual penal** / Guilherme de Souza Nucci. – 17. ed. – Rio de Janeiro: Forense, 2020

NUCCI, Guilherme de Souza. **Manual de processo penal e execução penal**. 12.º edição. Ed. Forense. Rio de Janeiro.

NORTON, **Como reconhecer e se proteger contra o crime cibernético**, Disponível em < https://br.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html> acesso em 20 de dezembro de 2020

PINHEIRO, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010

REDE EAD-SENASP. Ministério da Justiçae Cidadania. Secretaria Nacional de Segurança Pública. **Crimes Cibernéticos** –Procedimentos Básicos, 2015.

SILVA, Marco Antônio Marques da Silva. **Acesso à Justiça Penal e Estado Democrático de Direito**. São Paulo: Ed. J. de Oliveira, 2001, p. 07

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. ***Crimes Cibernéticos, Ameaças e Procedimentos de investigação***. Rio de Janeiro: Brasport, 2013