FACULDADE DAMAS DA INSTRUÇÃO CRISTÃ
CURSO DE DIREITO

DENAYDE RODRIGUES DE SANTANA

SISTEMA DE PROVAS NOS CRIMES VIRTUAIS

Os desafios da instrução probatória em ações penais relativas aos crimes virtuais no Brasil.

Recife
2019

DENAYDE RODRIGUES DE SANTANA

SISTEMA DE PROVAS NOS CRIMES VIRTUAIS

Os desafios da instrução probatória em ações penais relativas aos crimes virtuais no Brasil.

Monografia apresentada à Faculdade Damas da Instrução Cristã como requisito parcial para obtenção do título de Bacharel em Direito

Área de Concentração: Direito Processual Penal
Orientador: Prof. Dr. André Carneiro Leão

Recife
2019

Catalogação na fonte
Bibliotecário Ricardo Luiz Lopes CRB/4-2116

Santana, Denayde Rodrigues de.
S232s Sistema de provas nos crimes virtuais: os desafios da instrução probatória em ações penais relativas aos crimes virtuais no Brasil / Denayde Rodrigues de Santana. - Recife, 2019.
86 f.

Orientador: Profº. Dr. André Carneiro Leão.
Trabalho de conclusão de curso (Monografia - Direito) – Faculdade Damas da Instrução Cristã, 2019.
Inclui bibliografia

1. Direito. 2. Cibercrime. 3. Autoria. 4. Prova. I. Leão, André Carneiro. II. Faculdade Damas da Instrução Cristã. III. Título

342.3 CDU (22. ed.) FADIC (2019.1-257)

FACULDADE DAMAS DA INSTRUÇÃO CRISTÃ
CURSO DE DIREITO

DENAYDE RODRIGUES DE SANTANA

SISTEMA DE PROVAS NOS CRIMES VIRTUAIS: Os Desafios da Instrução Probatória em Ações Penais Relativas aos Crimes Virtuais no Brasil.

Defesa Pública em Recife,_____ de_____de_____.

.

BANCA EXAMINADORA:

Presidente:
_____.

Examinador(a)
_____.

DEDICATÓRIA

Ao autor da minha fé, o Pai que em todos os momentos me concedeu sua graça, a quem eu dedico todo o meu viver, JESUS.

AGRADECIMENTOS

Momento mais difícil, pois nessa jornada de seis anos e meio, houve alguns percalços como desistência de um período e troca de Faculdade, mas em fim acabou essa etapa.

Primeiramente a minha família e meus amigos, peço desculpas por não ter dedicado mais tempo a vocês, vida de estudante de Direito não é fácil, requer dedicação ao estudo, e deixei muitas vezes de lhes dar atenção, de estar presente. Mas saibam que minha prioridade sempre será vocês, e minhas vitórias sempre serão para vocês.

Álvaro, filho querido. Tu és a melhor maneira de definir o que é Amor. Esse ano começa a sua jornada na vida acadêmica superior, #orgulho. Agora é com você passar por esse estágio no jogo da vida.

A meu Esposo, Fabiano obrigada por segurar toda a barra nos momentos da minha ausência, obrigada pelo incentivo, por ficar feliz quando estou feliz e de se entristecer quando fico triste. Companheirismo é tudo que uma mulher necessita pra ser feliz e eu sou muito feliz por ter você.

A minha Mãe Elza, sempre me incentivou a crescer como mulher, ser independente e conquistar o meu papel no mundo.

A meu Pai Adauto que não está vendo essa etapa ser concluída, mas sei que seria um orgulho para ele. Estarás sempre em meu coração, e o prazer do conhecimento herdei de você.

A minhas irmãs Dayse, incentivo desde que me entendo por gente. Leia, estude, essas eram as frases, e Denise que sempre me viu como pequena e que me incentivava com a frase;Eu duvido tu fazer! Tu não sabes!

A minha sogra Maria, saudades que chega a doer. Obrigada por todo apoio.

Família, não teria conseguido sem vocês ao meu lado.

Sentirei saudades de todas as turmas que já passei, e foram muitas nesses anos de curso, de todos os colegas de sala que de alguma forma contribuíram com a construção do meu conhecimento.

Agradeço a todos os funcionários da secretaria, os quais, sempre me ajudaram quando perdida estava, vocês quem fazem a Faculdade prosperar.

Aos funcionários da biblioteca que me auxiliaram encontrando livros que necessitava, separando alguns exemplares nas matérias que precisava e pela torcida em cada etapa que concluía.

Aos funcionários da portaria e segurança, como também aos contribuintes da limpeza, a Faculdade não seria nada sem o vosso trabalho.

Obrigada a Todos os Professores da Faculdade Marista onde comecei, e aos Professores da Faculdade Damas, onde concluir.

Agradeço ao orientador o Professor André Carneiro Leão, a admiração por você é imensa, obrigada pela contribuição na minha monografia.

Momento ESPECIAL, Professor Ricardo Silva sem você não teria conseguido, obrigada por tudo. Nos encontraremos no Universo dos games.

A Victor Medeiros, primeira pessoa que me acolheu na faculdade Damas, desculpas pelos aperreios como, me envia o material! O professor deu qual assunto?O que vai cair na prova? Entre tantos, você nunca me deixou na mão. Valeu criança generosa. ‘Da facul pra vida toda”.

A todos que torceram por mim. Muito Obrigada.

RESUMO

As inovações tecnológicas atingem diretamente a instrução probatória em face aos crimes virtuais. Com a expansão da internet e o uso dos aparelhos eletrônicos como computadores, *smartfones, tablets*, facilitou a vida pela praticidade em obter informações, comunicar-se, negociar, entreter entre inúmeras atividades que podem ser exercidas sem sair de casa. O Direito tem seu papel fundamental nessas interações sociais, portanto, tem o dever de ser atual e adequado, se mostrando eficaz em todas as áreas a ele conferidas. Trataremos nesse estudo das dificuldades encontradas no que diz respeito aos crimes virtuais, pontuando como os crimes se proliferam na rede e como é ação do poder Estatal em razão desse novo tipo de delito. Utilizando para desenvolver o trabalho a metodologia dogmático-jurídica, e o método analítico hipotético-dedutivo. A problemática a ser discutida foca os encalços probatórios em solucionar os crimes na rede, demonstrando a dificuldades encontradas na identificação da autoria, no recolhimento das provas materiais e nas leis brasileiras que regem a matéria. Tentaremos apontar uma solução a fim de proteger o cidadão e punir o cibercriminoso.

Palavras-chave: Crime, Prova, Internet, Cibercrime, Virtual, Autoria.

ABSTRACT

Technological innovations directly affect evidentiary education in the face of virtual crimes. With the expansion of the internet and the use of electronic devices such as computers, smartphones, tablets, it made life easier for information, communication, negotiation and entertaining activities that can be carried out without leaving home. Law has a fundamental role in these social interactions, therefore, it has the duty to be current and adequate, proving effective in all areas conferred upon it. In this study, we will discuss the difficulties encountered in relation to virtual crimes, stating how crimes proliferate in the network and how it is the State's power because of this new type of crime. Using to develop the work the legal-dogmatic methodology, and the hypothetical-deductive analytical method. The problematic to be discussed focuses on the probe in solving the crimes in the network, demonstrating the difficulties found in the identification of authorship, in the collection of material evidence and in the Brazilian laws that govern the matter. We will try to point out a solution in order to protect the citizen and punish the cybercriminals.

Keywords: Crime, Proof, Internet, Cybercrime, Virtual, Authorship.

SUMÁRIO

1 INTRODUÇÃO

A modernidade do século XXI trouxe consigo as vantagens da comunicação instantânea e as desvantagens com a invasão de privacidade. Esse conjunto de evoluções tecnológicas e essa modernidade tornam-se ainda mais perceptível com o avanço da rede mundial de computadores conectados à internet, criando uma série de problemas sistêmicos no âmbito jurídico.

Com movimentações inimagináveis e incalculáveis, as deflagrações de fatos, notícias e novas modalidades criminosas multiplicam-se,criando a todo instante novas maneiras de cometer delitos e isentar-se de culpa.Assim, os crimes virtuais se espalham em cadeia, com rapidez exorbitante e propagações devastadoras, com um simples aparelho eletrônico conectado à internet.

O Direito é um instrumento regulador dos conflitos sociais, econômicos e políticos, por isso, cabe a ele acompanhar as mudanças tecnológicas com intuito de solucionar as peculiaridades trazidas por novas práticas criminosas.

Essa tecnologia em movimento afetou de forma singular o cidadão, que tem a sua privacidade burlada, invadida e saqueada de diversas maneiras. Convive com a nítida sensação de estar aprisionado pelo sistema virtual. Do outro lado da tela está o sujeito que comete tal modalidade de crime, sujeito esse, anônimo, que restaura a identidade virtual numa constância paulatina e dificulta à busca por provas conclusivas.

A legislação não evoluiu como a velocidade em que se propaga o mundo tecnológico, isso eleva o poder dos criminosos pela dificuldade da investigação. Essa dificuldade não está diretamente atrelada ao âmbito material da esfera jurídica, mas o real e devastador problema em nosso ordenamento é o próprio legislativo com questões políticas que deixam o composto legal travado. A hipótese desse trabalho foca em uma solução que possibilite a identificação do cibercriminoso, visto que, nesse tipo de delito é a maior dificuldade encontrada pelo Estado.

A vida privada, o patrimônio, a propriedade material e intelectual, os costumes, as famílias, a fé, o sentimento religioso, a administração pública, são constantemente afetados por esse tipo de delito, portanto, a sociedade e o poder público devem andar juntos para solucionar esses conflitos.

A proposta do tema é evidenciada ao longo da explanação do presente trabalho, que usa a metodologia dogmático-jurídicos, o estudo reporta o Direito Penal e Processual Penal, focando nas leis específicas voltadas ao conteúdo virtual, levantando os conceitos gerais de como essas provas se comportam perante o processo. e tem por método analítico o hipotético-dedutivo, a pesquisa foi construída com o auxílio de artigos acadêmicos, revistas, *sites*, livros e a jurisprudência brasileira e internacional, atribuído a amplitude do crime.

O primeiro capítulo deste trabalho define os crimes virtuais e os desafios que esse crime traz para o sistema penal material. Destacando o conceito, a evolução histórica, os crimes de informática e de computador, a conduta do agente e as leis vigentes no nosso ordenamento. O segundo capítulo descreve os parâmetros da instrução probatória no Brasil, abordando para melhor compreensão o conceito de provas, a historicidade e evolução das provas, as características das provas, os meios de prova e o sistema brasileiro de provas.

No terceiro capítulo o objeto específico entra no seu núcleo, neste capítulo analisamos os desafios e as soluções apontados pela doutrina para identificar a autoria. Destrinchando fatos inerentes as inovações no sistema de coleta e apreciação de provas, as dificuldades da identificação da autoria, uma vez que, nesse tipo de crime o ambiente virtual proporciona o anonimato, a necessidade de uma polícia investigativa atualizada e especializada nessa área e as possíveis soluções dentro do nosso ordenamento. Trouxemos também, o projeto de lei ainda em tramitação no parlamento brasileiro, que tem o foco na busca de soluções de prevenção e combate em frente aos crimes virtuais.

A presente monografia tem por pontuar as particularidades que decorrem dos crimes virtuais, com o objetivo maior de identificar os desafios apontados na doutrina, no que diz respeito à obtenção de provas a fim de comprovar a autoria, as dificuldades enfrentadas pela perícia forense e a legislação vigente brasileira.

Por fim, cabe ressaltar que a presente monografia não pretende exaurir todas as soluções que corroboram para suprir os problemas dos crimes na internet, mas, apontar os desafios da instrução probatória na justiça brasileira diante esse tipo incriminador tão atual e desafiador.

2 CRIMES VIRTUAIS

Os crimes virtuais são condutas ilegais praticadas por pessoas que se utilizam os meios digitais de comunicação e acesso à informação, para cometer delitos.

Com o avanço tecnológico e um exponencial aumento do uso de dispositivos informatizados conectados a internet, da grande quantidade de informação a apenas um toque, verifica-se uma grande alteração nos comportamentos sociais, assim como o avanço de novos delitos. Os crimes virtuais são contemporâneos ao avanço tecnológico, ampliando a relevância para a prática da conduta ilícita [1].

Simultaneamente com o uso desenfreado de tecnologia é notável que, nos últimos anos não apenas melhorou os padrões de vida mundial, mas também facilitou a consecução de diversas modalidades criminosas alterando as diferentes formas de desvios de conduta, tendo como meio os dispositivos eletrônicos para a prática do ilícito.

No decorrer desse capítulo trataremos do crime virtual, abordado a sua definição, historicidade, características e diferenças naatuação do criminoso no meio informático. Especificando no último subitem a sua evolução em frente ao Legislador brasileiro.

2.1 Conceito, Historicidade e Características dos Crimes Virtuais

O homem desde os primórdios cria ferramentas que auxiliam seu cotidiano. Assim, podado nessa evolução as mais variadas formas de tecnologias foram desenvolvidas. Uma crescente evolução que ficou ainda mais evidenciada na última década com a criação da internet.

Essa verdadeira revolução tecnológica proporcionou a interação dos indivíduos, tornando-o parte ativa e passiva ao mesmo tempo quando se dispõe no mundo virtual. Dentro da rede, se perde a noção do mundo real no sentido do “aqui e agora”, pois o tempo real ultrapassa os limites territoriais e transcende o devido espaço/tempo.

---

[1]MALAQUIAS, Roberto Antônio Darós. **Crime Cibernético e Provas** - A investigação criminal em busca da verdade. Curitiba. Editora Juruá, 2012, p.52.

Concomitantes com a criação da internet vieram os crimes virtuais, chamados também de crimes digitais, cibercrime, crime de rede, crime de informática ou crimes cibernéticos. Apresentando-se como crimes que utilizam algum meio informatizado ligado ou não a uma rede para cometer o ilícito.

Gustavo Correa define que: “Crimes cibernéticos são todos aqueles delitos vinculados as informações armazenadas ou em trânsito por computadores, que são utilizadas ilicitamente para fraudar ou mesmo ameaçar as vítimas” [2].

O meio eletrônico é a ferramenta usada para cometer o ato ilícito, portanto, o crime virtual seria um crime meio, neste sentido define Patrícia Peck Pinheiro “O crime virtual é, em princípio, um crime de meio, ou seja, utiliza-se de um meio virtual, para cometer o delito”[3].

Atecnologia tem auxiliado o homem a evoluir, ao mesmo tempo facilitou a prática dos meios delituosos. Nas palavras de Thomas Welch “É notório que as mesmas novas tecnologias que permitiram o avanço e a automação de processos de negócio, também abriram as portas para muitas novas formas de uso indevido de computadores” [4].

É diante dessa conjuntura que o ordenamento jurídico brasileiro precisa acompanhar, estar a frente da realidade social da “era digital”, estabelecendo uma adequação para dar maior eficácia na preservação do indivíduo e na segurança da informação, abordando temas como o da legítima defesa da internet e a necessidade da preservação de provas eletrônicas.

Não é fácil para o legislador acompanhar as novas formas de conduta, talvez, seja inviável prever as múltiplas transformações tecnológicas, caracterizando, sobretudo, a velocidade da transmissão dessas informações. O aplicador do Direito apresenta essa mesma dificuldade diante da ausência de norma reguladora.

O crime virtual tem repercussão mundial, essa nomenclatura Cibercrime tem derivação da palavra americana *Cybercrime*, que é constituída por duas palavras distintas;*Cyber+Crime. O* significado da palavrada palavra *Cyber* é o diminutivo de *Cybernetc,* que em português significa coisa ou local que possui uma concentração

---

[2]CORREIA, Gustavo Testa. **Aspectos Jurídicos da Internet**. São Paulo: Editora Saraiva, 2000, p.346.
[3]PINHEIRO, Patrícia Peck. **Direito Digital**. São Paulo: Editora Saraiva, 2013, p. 208.
[4]WELCH, Thomas. Computer Crime Investigationand Computer Forensics. *In*: TIPTON, Harold; KRAUSE, Micki (Org.). **Information Security Management Handbook.** 6th ed. Florida: Auerbach Publications, 2007, p. 2782-2782.

de tecnologia avançada, em especial computadores, internet, banco de dados, poderá também ser traduzida por espaços virtuais[5](tradução nossa).

Como toda relação processual penal os sujeitos do cibercrime se divide em: sujeito ativo (o criminoso), e o sujeito passivo (a vítima).

O sujeito ativo é aquele que diretamente comete conduta ilícita e culpável, da mesma maneira que no crime comum “mundo físico”, essas condutas terão de ser típicas e antijurídicas e que o sujeito que praticou tenha capacidade jurídica para ser penalizado.

Existem termos técnicos que são usados a fim de diferenciar o sujeito ativo do crime virtual. Uma nomenclatura que é logo associada quando falamos em cibercriminoso é o termo *Hackers,* entretanto esse termo é específico para sujeitos que invade uma máquina conectada a uma rede, sem autorização dos donos, um invasor que se utiliza o meio virtual para roubar informações com intuito de levar vantagem ou apenas lesar a vítima.

Os *Phreakers* são indivíduos que dispõe de informações de terceiros, por meio telefônico e sem autorização, podendo usar as informações obtidas para chantagear as suas vítimas.

E por fim, os *Pirates* determinados por indivíduos que reúnem e distribuem *softwars* (programas) protegido por *copyright* (direito autoral), e utiliza desses programas como se fosse seu[6].

O sujeito passivo do cibercrime é o sujeito igualmente como nos crimes comuns, definido como aquele a quem recai a ação ou omissão do delito. Podendo ser pessoa física ou jurídica.

O termo cibercrime, foi mencionado pela primeira vez em uma reunião na França no ano de 1999, por um subgrupo do G-8. Esse grupo era composto pela Rússia, pela sua importância militar e histórica, e os sete países mais ricos do mundo, e o foco principal dessa reunião, era analisar as maneiras e os métodos usados para combater os crimes no meio virtual.

Dessa convenção em Lyon(França), iniciou uma série de conversas e assim deu início a um conselho Europeu, que propôs um esboço da primeira convenção

---

[5]INFOPEDIA. 2006. **Cibercrime**. Disponível em: https://www.infopedia.pt/dicionarios/lingua-portuguesa/cibercrime. Acesso em: 09 abr.2018.

[6]E-GOV. 2004.**Diferença Entre *Hackers*, *Phreakers* e *Pirates*.**.Disponível em: http://www.egov.ufsc.br/portal/conteudo/saiba-diferen%C3%A7a-entre-hackers-crackers-white-hat-black-hat-gray-hat-entre-outros. Acesso em: 02 mai. 2018.

sobre o cibercrime.No ano seguinte em 2000, incorporou um conjunto de técnicas de vigilância consideradas necessárias na luta contra os crimes virtuais[7].

Em 2001, houve a primeira Convenção em Budapeste (Hungria)que tratava especificamente dos crimes cibernéticos, à qual, só entrou em vigor a partir de julho de 2004, o objetivo da convenção era conceituar alguns termos específicos, como fornecedor/provedor de serviços, sistemas e dados informático, o direito penal e processual penal no âmbito internacional, e ainda da competência e cooperação internacional entre os Estados membros.

Conjuntamente, com todos esses assuntos abordados na convenção também foi discutida a soberania constitucional de todos os países, observando sempre, os princípios gerais do Direito de cada um deles, exigindo a conservação das normas e tratados dos Direitos Humanos Internacionais[8].

A preocupação de grande parte dos países se caracteriza, por ser esse sistema mundialmente interligado e disponível para uso individual. Um sistema sem fronteiras internacionais, onde existe total liberdade não ditando uma forma de utilização exata e precisa, portanto, todo indivíduo do mundo tem potencial de ser vítima ou criminoso

Chamado de *Internacional-Networking* ou apenas Internet, é uma rede interligada em um espaço virtual onde são trocadas as mais variadas informações em um espaço infinito, uma sociedade paralela ao real onde há uma organização por meio cooperativo, Anastásio Dullius define dessa forma a internet como:

> Uma sociedade cooperativa que forma uma comunidade virtual, estendendo-se de um extremo a outro do globo. Como tal, a internet é um portal para o espaço cibernético, que abrange um universo virtual de idéias e informações em que nós entramos sempre que lemos um livro ou usarmos um computador[9].

---

[7]KAMINSKI, Omar. 2010 **Tratado Internacional contra crimes na Internet.** Disponível em: https://www.conjur.com.br/2001-nov-24/convencao_lanca_tratado_internacional_cibercrimes#author. Acesso em:24 ago. 2018

[8]BARBUENA, Lucas André. **Crimes Cibernéticos.** Publicado em 24 Mar. 2018. Disponível em: https://lucasbarbuena.jusbrasil.com.br/artigos/559759168/crimes-ciberneticos. Acesso em: 20 mar. 2019.

[9]DULLIUS, AladioAnastacio; HIPPLER, Aldair; FRANCO, Elisa Lunardi. **Dos Crimes Praticados em Ambientes Virtuais**. Santa Rosa, 2012. Disponível em: http://www.conteudojuridico.com.br/artigo,dos-crimes-praticados-em-ambientes-virtuais,38483.html. Acesso em: 14 abr. 2018.

Para Tanembaum “Internet é um conjunto de computadores autônomos interconectados por uma única tecnologia” [10].

Inicialmente a internet foi criada estritamente com o objetivo de integrar as investigações e a comunicação entre os militares e o setor de inteligência das universidades, surgiu por volta dos anos 60, veio a partir de um projeto da agência Norte-Americana *Advanced Researchand Projects Agency* (*ARPA),* com o objetivo de conectar os computadores dos seus departamentos de pesquisa ao Instituto de Pesquisa de Stanford e a Universidade de *Utah*, criando assim a *ARPANET (Advanced Research Projects Agency Network).*

Ao longo da história da internet, foram criados alguns sistemas dando estrutura a esse universo, em 1983,deu início ao *Internet Activities Board (IAB)*(conselho de atividades) ou *Architecture Board* (conselho de Arquitetura) como é conhecido, forma a arquitetura que sustenta essa rede. Mais tarde,em 1989 com a evolução dessa estrutura veio a ser a*(IRTF)Internet Research Task Force*ou *(IETF) Internet Engineering Task Force* (Força-Tarefa de Pesquisa da Internet). Centros que deram sustentação a essa rede tecnológica até os dias de hoje.

Os centros acadêmicos também não pararam as suas pesquisas, ao longo do tempo desenvolveram maneiras de avançar essa rede. Deste modo, nasceu em 1986 a Fundação de Ciência Nacional (NSFNET*),* instituição voltada ao uso da internet e responsável pela expansão das ligações a qual abriu caminho para que a internet deixasse de ser exclusiva de uso militar.

A busca por novas tecnologias em comunicação era tão necessária e apreciada que essa pesquisa passou a ser mantida com apoio das organizações IBM, MCI, que eram empresas de telecomunicações, e a *MERIT* instituição responsável pela rede de computadores de instituições educacionais do Estado do *Michigan*, que formaram uma associação conhecida como *Advanced Networkand Services (ANS)*dando ensejo a uma organização sem fins lucrativos, com a intenção de executar a expansão da estrutura da rede mundial de telecomunicações[11]*.*

Desse avanço nas pesquisas por vota de 1993, a internet deixou de ser uma instituição de natureza apenas acadêmica passando a ser explorada comercialmente, houve uma reestruturação e uma nova espinha dorsal (*backbones)*

[10]TANENBAUM, Andrew S.**Redes de Computadores.**Brasil.Editora**,**Elsevier. 2003, p.19.
[11]TANENBAUM,Andrew S.op. cit.,p. 42-45.

foi criada, e é essa nova estrutura que constitui a estrutura da internet como é hoje, a maior parte dominada por empresas privadas.

Atualmente a internet obedece a uma tecnologia de rede individual, conceito chave de arquitetura aberta, que é escolhida pelo provedor que está sendo contratado, mas permanece ainda conectado com outras redes através da arquitetura de *Internetworking.* Essa nova estrutura faz com que cada um desses provedores tenha a sua interface desenvolvida de acordo com quem utiliza o serviço, passando assim a individualizar a sua própria forma de conexão[12].

Conseguinte, esse mundo virtual é um meio democrático onde organizações privadas, universidades e agências governamentais sustentam ou "controlam" parte desse mundo, cada um agindo como administrador, controlando a sua própria rede e colaborando entre si para dirigir o tráfego de informações.

Concomitantemente com a criação da internet pra uso civil é a criação do cibercrime, por ser a interface desse sistema um mundo incalculável, onde não há controle cabível de comando pelos provedores e pelo poder estatal. Então o conteúdo produzido nesse ambiente fica a cargo de quem utiliza, e não de quem o disponibiliza.

Dessas muitas nuances existentes pelos meios convencionais de uso dentro do universo virtual, o conteúdo lícito que é produzido chega a ser irrisório diante do conteúdo ilícito que se mostra em uma interface paralela. O conteúdo existente no submundo da internet trazendo uma melhor compreensão faz-se um paralelo como um grande *Iceberg*, onde vemos a superfície pequena (internet convencional) comparado com o maior conteúdo que é encoberto pelo mar (internet não convencional).

Todo esse universo paralelo tem sua estrutura "organizada", com denominações e terminologias próprias e com uma estrutura dorsal bastante avançada. Esse universo é denominado por *Deep Web* (teia oculta) primeiramente atribuído a Michael K. Bergman, *CEO* e cófundador da *Structured Dynamics LLC* quem primeiramente utilizou esse termo, referindo-se a todo conteúdo que não pode ser indexado pelos sites de busca, dessa forma não está disponível diretamente para quem navega convencionalmente na internet[13].

---

[12]WAZLAWICK, Raul, **História da Computação.** Brasil. Editora: Elsevier. 2016, p. 26.
[13]WAZLAWICK, Raul, op. cit., p. 29.

Nessa estrutura oculta existem *sites*, fóruns e comunidades que não ganham páginas específicas, e quando pesquisadas nos *sites* de busca convencionais não ficam visíveis por não possuir endereço fixo. Esses endereços encontram-se pairando em um mundo oculto, podendo ser enxergado através de chaves criptografadas, indexadas a sites específicos obtendo uma real proteção desses conteúdos.

O cibercriminoso utiliza essa ponte, de um lado as informações relevantes e lícitas, e do outro lado um universo de possibilidades, abrindo um novo mundo para os mais variados delitos. Leonardo Pereira diz em seu artigo que.

> A *Deep Web* é considerada a camada real da rede mundial de computadores, comumente explicada em analogia a um iceberg: a internet indexada, que pode ser encontrada pelos sistemas de busca, seria apenas a ponta superficial, a "*surface web*". Todo o resto é a *Deep Web* - não à toa o nome que, em inglês, significa algo como rede profunda. “Essa parte de baixo do iceberg existe por causa das deficiências da parte de cima, por causa do uso comercial excessivo da parte de cima[14].

O cibercriminoso utiliza a *Depp Web* com o objetivo de usufruir o que esse universo proporciona, dentro dessa teia oculta existem drogas, pedofilia, zoofilia, matadores de aluguel, armas, como também serviços privados(sexuais), vendas de produtos, programas, sistemas de pesquisa avançada para quem trabalha na área informática e afins.

A procura pelo conteúdo da *Depp Web* é justificada, pois proporciona privacidade, o usuário se esconde dentro dessa teia de informações com criptografia avançada com a ilusão de manter-se anônimo. Usando esse universo paralelo para manter a privacidade. O usuário não acessa a *Depp Web* apenas na intenção de adquirir produtos ilícitos, até mesmo porque, dentro dessa rede existem materiais lícitos. O prazer de acessar um universo paralelo com conteúdo específico e com altos padrões em sistema computacional e tecnológico faz com que exista um número imensurável de usuários.

A dificuldade de encontrar essa rede paralela permanece, pois, para ter acesso é necessário obter conhecimento em computação.Navegar dentro da *Depp Web* e chegar aos conteúdos ilícitos, somente será possível se o usuário tiver

[14]PEREIRA, Leonardo. ***Deep web*:** saiba o que acontece na parte obscura da internet. Olhar digital, 2012. Disponível em: https://olhardigital.com.br/fique_seguro/noticia/deep-web-saiba-o-que-acontece-na-parte-obscura-da-internet/31120. Acesso em: 12 mar.2018.

conhecimento em códigos criptografados, barrando o acesso ao usuário comum, o Estado e os Provedores da Internet[15].

Nessas múltiplas faces do mundo virtual, existe ainda algo mais complexo e obscuro responsável pela maioria dos mitos conhecidos na *DeepWeb, a DarkWeb,*o território mais profundo da Internet*,* com uma criptografia ainda mais avançada e complexa, somente alcançadas por pequeno grupo de usuários especialistas em informática avançada.

> Em sua estrutura completa é análogo a imagem de um Iceberg. A parte visível deste é denominada de *SurfaceWeb* enquanto sua parte imersa simboliza a *Deep Web*, representando diversos aspectos que diferenciamos ciberespaço. Um exemplo dessa discrepância se dá nos navegadores específicos usados para ambos. *Softwares* conhecidos como o Google *Chrome* e o Firefox, enquanto específicos da *Surface Web*, não conseguem captar o conteúdo da *Deep Web* em que são utilizados navegadores como o TOR[16].

Esse universo profundo utiliza de letras e de números aleatórios, secretos e não confirmados os quais exigem alterações do *hardware*, para que, possíveis comunicações ocorram, um mundo complexo o bastante, encobrindo o nível mais alto de conteúdo ilícito, facilitando a atuação do cibercriminoso pela dificuldade que proporciona a identificação.

Compreendendo a maneira que o cibercriminoso utiliza para cometer delitos, observa-se também, que a característica específica do cibercrime é a utilização do meio virtual, de um ambiente informatizado ligados a uma rede ou a utilização de alguns dispositivos eletrônicos, na doutrina brasileira esse tipo de delito é denominado por crimes convencionais.

Vicente Greco explica o que seriam crimes convencionais no âmbito virtual:

> Focalizando-se a Internet, há dois pontos de vista a considerar: crimes ou ações que merecem incriminação praticados por meio da Internet e crimes ou ações que merecem incriminação praticados contra a Internet, enquanto bem jurídico autônomo. Quanto ao primeiro, cabe observar que os tipos penais, no que concerne à sua estrutura, podem ser crimes de resultado de conduta livre, crimes de resultado de conduta vinculada, crimes de mera conduta ou formais (sem querer discutir se existe distinção entre estes) e crimes de conduta com fim específico, sem prejuízo da inclusão eventual de elementos normativos. Nos crimes de resultado de conduta livre, à lei

[15]DA SILVA ALMEIDA, J.; Roque, B. V. S. ***ChallengesOf The Law In The Regulation:*** *Of Legal Relations In Deep Web And Cyber Crimefigshare*, 9 fev. 2018. Disponível em: https://figshare.com/articles/challenges_of_the_law_in_the_regulation_of_legal_relations_in_deep_web_and_cyber_crime/5873892/1. Acesso em: 29 mar. 2019, p. 164.
[16] DA SILVA ALMEIDA, J.; Roque, B. V. S. op. cit., p. 166.

> importa apenas o evento modificador da natureza, com, por exemplo, o homicídio. O crime, no caso, é provocador o resultado morte, qualquer que tenha sido o meio ou a ação que o causou[17].(grifos nosso)

No Brasil, o Centro de Estudos, Respostas e Tratamentos de Incidentes de Segurança no Brasil (CERT.br) grupo vinculado ao Comitê Gestor da Internet no Brasil, realizou uma pesquisa apontando que no ano de 2018 foram totalizados 676.514 incidentes só no Brasil, com os mais diversos tipos de crimes como ataques a servidores Web, propagação de códigos maliciosos e tentativas de fraudes.

Os crimes virtuais obtiveram um aumento considerável devido ao uso do computador individual. Os computadores domésticos, aparelhos eletrônicos e a expansão da internet, deixaram os indivíduos mais vulneráveis a sofrerem ataques facilitando a ação de criminosos.

2.2 Classificação dos Cibercrimes

Se comparado com a rapidez em que a tecnológica a doutrina jurídica anda em passos pequenos, ainda mais quando trata das classificações dos cibercrimes. A gama de crimes diversificados e as novas práticas deixam obsoletas quaisquer classificações, pela velocidade das modificações nas formas de praticar o ilícito.

Ivette Senise Ferreira sugere um norte para uma possível classificação dos crimes virtuais:

> Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial[18].

Como não há uma consolidação na acerca de uma classificação específica e igualitária, a classificação dominante é a que divide os cibercrimes em Próprios, Impróprios, Mistos, Comuns e Puros.

Essa classificação em próprios e impróprios e mistos, não se confunde com a classificação já existente no direito penal que utiliza os termos próprios e impróprios para classificar os crimes segundo o sujeito ativo.

---

[17]GRECO FILHO, Vicente**. Algumas observações sobre o direito penal e a internet**. Boletim do IBCCrim. São Paulo. Ed. Esp., ano 8, n. 95, out. 2000.
[18]FERREIRA, Ivette Senise. **Direito & Internet:** Aspectos Jurídicos Relevantes. 2. ed. São Paulo: Quartier Latin , 2005, p. 261.

No universo virtual os crimes próprios são aqueles cometidos em cima dos dados e das estruturas físicas dos sistemas operacionais e dos programas de computador. São subdivididos em: 1. Crime Puro naquelas situações em que se faltar à condição especial exigida pelo tipo, tornando assim o crime atípico; 2. Crime Impuro, apresentado nas situações em que o agente desprovido da qualidade exigida pelo tipo responde por outro delito “São aqueles crimes em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizada[19].

Nesse raciocínio se posiciona Damásio de Jesus:

> Crimes eletrônicos próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informaçõese integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado[20].

Na categoria de crimes próprios há vários exemplos, fraudes eletrônicas, invasão de dispositivos informáticos, instalação de vírus, troca de senhas, modificação de aparelhos eletrônicos. O foco do cibercriminoso é precisamente os dados, softwares e dispositivos eletrônicos. Marco Túlio Viana aponta essa classificação como: “Aquelas em que o bem jurídico é protegido pela norma penal, atacando a inviolabilidade das informações automatizadas"[21].

Outra classificação é dada aos crimes cujo meio eletrônico é apenas uma das formas para cometer o delito, definidos assim por Crime Impróprio. Essa classificação determina que o uso do aparelho eletrônico seja só mais um meio de lesionar a norma, mas, não só através de aparelhos eletrônicos que o ato pode ser consumado.

Os crimes impróprios são praticados no meio virtual, contudo, ofendem o espaço físico real, recaindo sua ação sobre o patrimônio ou sobre a pessoa. No campo virtual esses crimes tomam forma, sendo amparados pelo Direito Penal, equiparando a sua aplicabilidade a norma jurídica igualmente aos crimes no campo real. Damásio de Jesus define os crimes impróprios como:

---

[19]VIANA, Marco Túlio,**Fundamentos de direito penal informático.** Do acesso não autorizado a sistemas computacionais**.** Rio de Janeiro: Forense, 2003, p. 13-26

[20]JESUS, Damásio Evangelista de. **Manual de Crimes Informáticos.** São Paulo: Saraiva, 2016, p. 218.

[21]VIANA, Marco Túlio apud CARNEIRO, Adeneele Garcia. **Fundamentos de direito penal informático.** Do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Forense, 2000, p. 65.

> Os crimes eletrônicos impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não computacionais ou diversos da informática[22].

Crimes que afetam o mundo real, mas utiliza o meio virtual pela facilidade que ele traz. Estelionato, fraudes, difamação, calúnia, *bullying* são considerados crimes dessa natureza.

Nas palavras de Ivette Senise Ferreira e Vicente Greco a classificação dada é a que dividem os crimes próprios como condutas praticadas contra o bem jurídico **informático**, e os crimes impróprios como as conduta praticada contra o bem jurídico **tradicional**[23](grifos nosso).

A classificação dada para crimes virtuais é quando a utilização dos meios eletrônicos é indispensável na prática do crime, chamados pela doutrina de Crimes Misto. A vítima é pessoa certa, sendo assim, o autor do crime direciona o ataque a uma determinada vítima a fim de obter vantagem em cima do patrimônio pessoal, a exemplo disso é a transferência sem autorização prévia, fraude bancária e quaisquer outros bens que possa ser retirado da vítima pelo cibercriminoso. “São delitos derivados da invasão de dispositivo informático que ganharam status de crime *sui genere*, dada a importância do bem jurídico protegido diverso da inviolabilidade dos dados” [24].

Finalizando, os crimes cibernéticos são delitos de natureza formal, posto que, se consumam no momento da prática da conduta delitiva, independente da ocorrência do resultado naturalístico. Vicente Maggio classifica como:

> Crime comum (aquele que pode ser praticado por qualquer pessoa), plurissubsistente (costuma se realizar por meio de vários atos), comissivo (decorre de uma atividade positiva do agente: “invadir”, “instalar”) e, excepcionalmente, comissivo por omissão (quando o resultado deveria ser impedido pelos garantes – art. 13, § 2º, do CP), de forma vinculada(somente pode ser cometido pelos meios de execução descritos no tipo penal) ou de forma livre (pode ser cometido por qualquer meio de execução), conforme o

[22]JESUS, Damásio Evangelista de. **Manual de Crimes Informáticos.** São Paulo: Saraiva, 2016, p. 116.
[23]FERREIRA, Ivette Senise. **A Criminalidade Informática.** Direito e Internet - Aspectos Jurídicos Relevantes. Editora Edipro, 2011, p. 202.
[24]JESUS, Damásio Evangelista de. **Manual de Crimes Informáticos.** São Paulo: Saraiva, 2016, p. 24

> caso, formal (se consuma sem a produção do resultado naturalístico, embora ele possa ocorrer)"[25].

A prática do ato já pode ser considerada crime, mesmo que não venha obter êxito, não sendo necessário alcançar o animus do autor.

2.3 Crimes de Informática

Manuel Lopes define a criminalidade informática, como: "Aquela que tem por instrumento ou por objeto sistema de processamento eletrônico de dados, apresentando-se em múltiplas modalidades de execução e de lesão de bens jurídicos"[26].

Rossini escreve com propriedade sobre o assunto, asseverando que a melhor denominação é aquela que leva o termo "informático" em sua composição:

> Ouso denominá-los "delitos informáticos", pois dessa singela maneira abarcam-se não somente aquelas condutas praticadas no âmbito da internet, mas toda e qualquer conduta em que haja relação com sistemas informáticos, quer de meio, quer de fim, de modo que essa denominação abrangeria, inclusive, delitos em que o computador seria uma mera ferramenta, sem a imprescindível "conexão" à Rede Mundial de Computadores[27].

A internet promoveu alterações nos bens jurídicos, os atingido com novos tipos de ações criminosas. A diferença é o que vivenciamos no mundo "real" se trata de algo que é palpável, enquanto no virtual se transforma no "irreal" por ser um território vasto e impossível de demarcação.

Diferente do que ocorrem com as condutas não informáticas onde o bem jurídico individual é atingido de forma mais explicita, o avanço da criminalidade na rede virtual fez com que o bem difuso ganhasse notoriedade. Partindo do pressuposto que há mais facilidade de atingir um número maior de pessoas em menos tempo, com menores números de agentes e menos recursos, obtendo os

---

[25]MAGGIO, Vicente de Paula Rodrigues. **Novo crime**: invasão de dispositivo informático - Disponível em: https://vicentemaggio.jusbrasil.com.br/artigos/121942478/novo-crime-invasao-de-dispositivo-informatico-cp-art-154-a. Acesso em: 20 nov. 2018.

[26]ROCHA, Manuel Lopes**;** GAMA Filho, Remy. **Crimes da Informática**. Editora: Copy Market. 2000, p.106.

[27]ROSSINI, Augusto Eduardo de Souza**. Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004, p. 125.

mesmos resultados, com o diferencial de maiores vantagens e de bônus o anonimato.

Diversas são as formas na qual um aparelho eletrônico pode ser invadido e atacado por criminosos. O conceito de crime informático tem sua especificidade baseada no uso da rede informática para cometer o delito, para Alexandre Daoune Gisele Truzzi crime informático é:

> Pode-se afirmar que a doutrina penal e os tribunais brasileiros têm adotado o conceito de crimes informáticos como ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão, definição esta, similar à que foi cunhada pela Organização para Cooperação Econômica e Desenvolvimento da ONU (Organização das Nações Unidas): "é qualquer conduta ilegal não ética, ou não autorizada, que envolva processamento automático de dados e/ou transmissão de dados[28].

O desempenho, destruir arquivos e se expandir, fazendo que o aparelho hospedeiro fique vulnerável a prática dos diversos crimes virtuais.

Um *Worm* (verme) é um programa auto replicante e completo, que uma vez hospedado poderá causar danos como deletar, transferir arquivoseenviar documentos por email,programa de tão maléfico que deixa qualquer computador vulnerável a ataques de terceiros.

Dentre os crimes informáticos, citaremos os mais frequentes consequentimente os mais conhecidos, isto é, os que atingem um número considerável de vítimas.

Cavalo de Tróiaé um deles, denominado assim pela comparação a mitologia grega, essa invasão se apresentam como programas normais, trazendo consigo o vírus escondido. Muito comum quando usuário faz um *downloads*, baixando um arquivo específico, o cavalo de tróia está embutido nesse arquivo, e a função é deixar a máquina vulnerável a ataques futuros.

Vírus é um programa cuja à intenção é infectar o sistema operacional da máquina que está sendo utilizada, tal como um vírus biológico (daí o nome), se instala em algum programa e se espalha fazendo cópias de si mesmo, tenta se proliferar em outros aparelhos informáticos. O objetivo do vírus é prejudicar o

[28]DAOUN, Alexandre Jean; LIMA, Gisele Truzzi de. **Crimes Informáticos:** o Direito Penal na Era da Informação. Disponível em: http://www.truzzi.com.br/pdf/artigo-crimes-informaticos-gisele-truzzi-alexandre-daoun.pdf. Acesso em: 30 mai. 2018.

desempenho, destruir arquivos e se expandir, fazendo que o aparelho hospedeiro fique vulnerável a prática dos diversos crimes crime virtuais[29].

Um *Worm* (verme) é um programa auto replicante e completo, que uma vez hospedado pode causar danos como deletar, transferir arquivo, enviar documentos por email sem autorização do usuário. O *worm* é um programa de tão maléfico que deixa qualquer computador vulnerável a ataques de terceiros.

Spam é uma mensagem não solicitada e enviada para um grande número de pessoas através do email. Originalmente da palavra inglês *spicehan* (presunto apimentado), no geral usado por empresas de propaganda para alcançar a massa, mas essas mensagens não desejadas podem estar infectadas por vírus, causando assim problemas no aparelho eletrônico.

Conhecido como *Spyware* (programa ou aplicativo espião), é um programa que recolhe informações sobre aquele que opera um computador infectado, e transmite essa informação para um terceiro. Um programa usado exclusivamente para espionar obtendo informações privadas do usuário.

Phishing caracterizado por fraude eletrônica, tendo o objetivo de adquirir informações de sigilo alto, atacando principalmente o ramo empresarial, e estatal. O *Phishing* se passa por empresa ou pessoa confiável através de mensagens eletrônicas para assim obter as informações sigilosas e de difícil acesso.

Botnet, são links em páginas confiáveis que uma vez acessados infectam o aparelho eletrônico, em geral estão anexadas em páginas acessadas por grande número de pessoa,seu objetivo é atingir uma quantidade maior de vítimas.

Rootkit consiste em, um conjunto de ferramentas que alteram a máquina do usuário infectado. O cibercriminoso tem o acesso remoto da máquina, tornando o aparelho eletrônico instável. Quase impossível de retirá-lo, pois, esse programa danifica o computador ou os arquivos[30].

Em virtude da existência de lacunas de norma especifica para a maioria dos crimes informáticos, e diante da impossibilidade de fazer uso da analogia *malam partem* no direito penal, resulta em certo benefício para o cibercriminoso. O cibercriminoso encontrou alguns métodos de se redescobrir, e realocar suas ações

[29]GETNINJAS. **Tipos mais Comuns de Invasão de Computador**. Disponível em https://www.getninjas.com.br/guia/assistencia-tecnica/computador-desktop/os-tipos-mais-comuns-de-virus-de-computador/ Acesso em: 26 abr. 2018.
[30]Idem.

onde não haja tipificações dos delitos por eles praticados. Nesse sentido Rogério Greco observa que:

> Em matéria penal, por força do princípio da reserva, não é permitido, por semelhança, tipificar fatos que se localizam fora do raio de incidência da norma, elevando-os à categoria de delitos. No que tange às normas incriminadoras, as lacunas, porventura existentes, devem ser consideradas como expressões da vontade negativa da lei. E, por isso, incabível se torna o processo analógico. Nestas hipóteses, portanto, não se promove a integração da norma ao caso por ela não abrangido[31].

Mesmo com todos os problemas da falta de tipos penais que sejam compatíveis com o crime virtual, a Internet não é uma terra sem lei. O Estado vem atuando de todas as formas para proteger o indivíduo e o interesse social.

Em decorrência da característica do "irreal" por não existir espaço físico, o cibercriminoso traça um paradigma imaginário, o sentimento de que não há como detê-lo, porém, o Direito Penal tema obrigação de oferecer uma proteção ao bem jurídico afetado, por exemplo, a informação individual e a segurança dentro da rede de computadores, protegendo a vida e o patrimônio.

A doutrina define como Crimes Puramente Informáticos, todos aqueles crimes que ainda não foram incluídos no nosso diploma Penal.

O acesso não autorizado a dispositivos de comunicação, a difusão de código malicioso, o crime contra o sistema de dados, pichação virtual e invasão de sites, são exemplos do que ainda falta ser amparado pelo sistema legislativo, mesmo com a Lei 12.965/14 muita coisa ainda terá de ser tipificada.

Diante disso, muitos indivíduos, com a mera intenção de bisbilhotar a vida alheia, cometem crime, pois o ato de invadir é amparado pela CF/88. A intimidade tem o aparato constitucional e devem ser preservadas, os criminosos aproveitam da rede para além de perscrutar, copiam dados, os modifica e até mesmo apagar esses dados retirando o do proprietário algo relevante ou íntimo, então, o aparato jurisdicional deve dar suporte, para impedir e punir esse tipo de invasão cibernética, em outras palavras Willian César Pinto de Oliveira diz que:

> Cabe destacar que a lei exige, como elemento subjetivo do tipo, a especial finalidade de obter, adulterar ou destruir dados ou informações. Assim sendo, se o agente invadir um computador apenas para ver as fotografias nele contidas, não incidirá no delito. [...] a lei exige "violação indevida de mecanismo de segurança", de sorte que, se o computador estiver ligado e

[31]GRECO, Rogério. **Curso de Direito Penal** – Parte Geral. 4. ed. Rio de Janeiro: Impetus. 2004, p. 48.

> não for exigida nenhuma senha, não haverá crime. Aliás, nesse tocante, pode-se entender que sequer houve invasão, já que se trata de um termo técnico que mereceria explicação[32].

Invasão sem que ocorresse furto ou roubo de senha e que não houve nenhuma modificação do conteúdo, só pelo fato de bisbilhotar poderá ser considerada invasão de privacidade.

O aparato constitucional visa proteger o cidadão, a interferênciano mundo econômico, social e político, interferem no âmbito jurídico, neste sentido é indispensável discutir, regulamentar e normatizar, o mundo virtual, obrigando assim, o Direito acompanhar as mudanças tecnológicas com o intuito de prevenir e dirimir os conflitos no ciberespaço.

Sobre a relação entre o Direito e a sociedade, Ada Pellegrini Grinover estabelece em sua obra que:

> Indaga-se desde logo, portanto, qual a causa dessa correlação entre sociedade e Direito. E a resposta está na função que o Direito exerce na sociedade: a função ordenadora, isto é, de coordenação dos interesses que se manifestam na vida social, de modo a organizar a cooperação entre pessoas e compor conflitos que se verificarem entre os seus membros[33].

Quanto mais cooperação social em face ao Estado, maiores chances terão de combater os crimes informáticos.

2.4 Crimes de Computador

Diferente dos crimes informáticos os crimes de computador traz consigo tipificação específica.

De todos os benefícios que a internet trouxe, vieram também os malefícios, pois o uso da tecnologia está ao alcance de qualquer cidadão. Os criminosos aproveitam do espaço para cometer os mais variados crimes, essa lista de tipos penais praticados na rede, é extensa, e quando o crime está devidamente tipificado no ordenamento jurídico configura-se crime de computador.

---

[32]OLIVEIRA, William César Pinto de. **Lei Carolina Dieckmann**. Disponível em: http://jus.com.br/revista/texto/23655. Acesso em: 12 jun. 2018.
[33]GRINOVER, Ada Pellegrini. **A Iniciativa Instrutória do Juiz no Processo Penal Acusatório.** Brasília, Revista Jurídica Consulex, nº. 169, Out. 2000, p.33-36,

Neste sentido, a nomenclatura pode não ser a mesma no mundo virtual, mas a configuração e tipicidade do crime são iguais as que já se encontram definidas na nossa legislação, a seguir arguiremos alguns tipos de crimes, analisando como se comportam no mundo virtual.

O Furto de Dados é quando o agente inicialmente prepara o terreno manipulando alguns programas específicos, como *spyware* ou um vírus na fase preparatória, e espera a oportunidade para conseguir o bem, fase executória, furtando dados da máquina do usuário.

A intenção do cibercriminoso é de consegui informaçõescomo senhas, poderão executar o crime. Com as senhas em mãos, o cibercriminoso poderá roubar e manipular dados pessoais e obter vantagem econômica (dinheiro) ou acessar informações sigilosas. Equiparado como o crime de furto descrito no Artigo 155 do Código Penal.

O Estelionato também é cometido na rede virtual igualmente como é no mundo real, definido como crime contra o patrimônio tem o comportamento no mundo virtual semelhante como no mundo real, estando tipificado no Artigo 171 do Código Penal, diferenciando apenas pelo *modus operadi*[34].A intenção é de obter vantagem econômica, induzindo a vítima ao erro, uma ação cometida de maneira direta e dolosa trazendo uma vantagem indevida para o criminoso.

A Pirataria Cibernética assim como no estelionato é o crime que recai contra a propriedade, a diferença é que na pirataria a propriedade é intelectual. No mundo virtual temos acesso a todo o tipo de conteúdo, a propriedade que antes era exclusivamente privada, mas com a internet passou a ser de "domínio público," no sentido da exposição que a propriedade é conhecida.

Nesse encalço do mundo moderno surge questões relativas aos direitos autorais, protegido pela Constituição art. 5º, XXVII dentre outros dispositivos jurídicos. Incidindo no ato de copiar e reproduzir obra que não é sua, a ciberpirataria ou pirataria cibernética recai sobre uma música, um livro, um trabalho acadêmico, até mesmo, sobre programas de computador, lesando o autor.

Outro crime bastante praticado no mundo virtual são os crimes contra a Honra, tendo previsão nos artigos 138, 139 e 140 do Código Penal e são inúmeros casos

[34]SIGNIFICADOS.com.br. Disponível em: https://www.significados.com.br/portugues/. Acesso em: 20 mar. 2019. Ás 15h42.

ocorridos no meio virtual, principalmente nas redes sociais. Os crimes contra a hora são os crimes de:

> 1-Crime de **Calúnia** que é quando se imputa falsamente a uma pessoa algo tipificado como crime; 2-A **Injúria** é a prática ofensiva a dignidade ou o decoro; 3- e a **Difamação** é quando imputa a outrem fato ofensivo à sua reputação[35].

A Pedofilia é um crime tipificado tanto pelo Código Penal artigo 234, quanto pelo Estatuto da Criança e do Adolescente, nos artigos (241-A/241-E), tem como objetivo promover sentimentos eróticos voltados à criança e ao adolescente, com uma diversidade de atos, como, distribuir, armazenar, expor, exportar, adquirir material erótico infanto-juvenil.

O uso de sistemas informatizados aumentou consideravelmente essa disseminação criminosa, com páginas e sites incentivadores à erotização. Prostituição e troca de arquivos, filmes e imagens voltados à exploração de sexual de crianças e adolescentes, o meio virtual também usado para sedução de menores configurando no crime de Estupro, art. 2013 do Código Penal.

O meio eletrônico como forma de comunicação e socialização elevou o potencial da interação mundial, mas também incidiu no aumento da criminalidade. Dentre esses aumentos delituosos as incidências do crime de Ameaça, previsto no Código Penal no artigo147. Os crimes de IntolerânciaReligiosa e Racismo, também obtiveram aumento, com um crescente número de autores, atingindo um maior número de vítimas, principalmente nas redes sociais.

O crime previsto no artigo 122 do Código Penal tipificado como induzir, instigar ou auxiliar alguém ao Suicídio, é disseminado constantemente na rede.

Finalizando, o crime de Tráfico de Drogas, artigo 33 da Lei 11.343 de 2006[36]esse crime tem uma própria maneira de agir no meio virtual, onde por meio da rede convencional e em principal da *Deep Web* poderá o usuário, comprar e vender as mais variadas drogas, auxiliado pela moeda virtual (*bitcoins*) e o anonimato que a rede proporcionou, agilizando as negociações.

---

[35]STRAZZI, Alessandra. **Crimes contra a honra** - diferenças entre calúnia, difamação e injúria, Disponível em : https://alestrazzi.jusbrasil.com.br/artigos/130177918/crimes-contra-a-honra-diferencas-entre-calunia-difamacao-e-injuria. Acesso em: 28 jun. 2018.

[36]BRASIL, **Lei nº 11.343**, de 23 de Agosto de 2006**.** Disponível em :http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11343.htm . Acesso em: 28 abr.2018.

Observando essas modalidades típicas e como elas ocorrem no mundo virtual, percebemos que o cibercrime com auxílio do computador e da internet, facilitou a realização dos mais variados delitos. Novas condutas atingem o bem jurídico a cada dia, e o que não havia sido atingido pela conduta criminosa ganhou força com a expansão dessa rede, portanto, existe uma necessidade de criação de mecanismos de repressão e prevenção, criando um direito específico que cuide desse novo mundo.

Nesses termos, a legislação brasileira vem adaptando o seu posicionamento, expandindo a interpretação das leis já existentes, e ampliando seu composto para o mundo virtual, com a finalidade de suprir a demanda.

2.5 A Legislação Brasileira e a Competência nos Crimes Virtuais

Todas as vezes que surge na sociedade algo relevante no cenário mundial, remete ao Direito uma proteção, tal qual, forautilizado nos primórdios da tecnologia quando surgiu o rádio, televisão, impressa e telefone, o Estado interviu cumprindo o papel detentor com regulamentação, adequação, e punição das condutas nocivas a sociedade, buscando um melhor modo para a preservação e manutenção de uma sociedade saudável.

Rodotá lista qualidades e particularidades necessárias para um ambiente jurídico adequado:

> Uma disciplina legislativa de base‘‘; _‘normas para casos específicos‘‘ ‘uma autoridade administrativa independente‘‘; _‘uma disciplina de recursos à autoridade judiciária‘‘ e _‘a previsão de um controle difuso, confiado à iniciativa de indivíduos e grupos[37].

Nossa Legislação vem se adequando a novos tipos de tecnologia, mas o mundo virtual é deveras rápido,sendo as modificações constantes e diárias.A burocracia politizada em que vivemos, acaba por fazer com que os efeitos da norma criada diante das situações cotidianas não cumpram o seu papel preventivo e punitivo pela rapidez das mudanças sociais e tecnológicas, contribuindo assim que as modificações feitas na norma acabam ficando obsoleta.

[37]RODOTÀ, Stefano. **A vida na sociedade da vigilância** - a privacidade hoje. Rio de Janeiro: Renovar, 2008. Tradução de: Danilo Doneda, Luciana Cabral Doneda, p. 87 - 88.

Nesse sentido, cita-se a colocação de José Luiz Bolzan de Morais e Elias Jacob de Menezes Neto:

> Um dos objetivos primordiais da *surveillance* é a previsão de comportamentos futuros, seja por parte do poder público em prever atitudes, seja pela iniciativa privada para prever quais as melhores formas de ganhar dinheiro com anúncios, exemplificativamente. O homem é um animal de hábitos, de maneira que, com a coleta de informações diversas durante período de tempo suficiente, é possível prever padrões de comportamento, deslocamento, preferências e interação social[38].

No entanto, a consagração legal desta proteção pode revelar-se insuficiente, pela quantidade de novos delitos.

A norma legal é pragmática quando fala que só podem ser considerados crimes aqueles que estejam de acordo com os princípios constitucionais, descrito no artigo 5°, XXXIX da Constituição Federal/88. Condutas que não estão tipificadas ou que foram formuladas sem a observância ao devido processo legal, não pode ser consideradas crime.

Atualmente existe um conjunto reduzido de normas tipificandocondutas no ciberespaço, portanto, uma lacuna se forma diante desse enorme mundo. As leis que impõe seu texto voltado aos crimes virtuais são a Lei Ordinárias 12.735/2012, 12.737/2012 e a Lei 12.965/2014.

A criação da Lei 12.737/2012 teve a sua base no projeto de lei 84/1999 que era, no entanto, rigoroso em garantias individuais.

A bancada governista criou uma lei opcional, determinado que as normas penais tipificassem as ações no universo virtual, também a criação de uma nova legislação que definiria direitos e deveres dos usuários da internet.

Sobre essa Lei Patrícia Peck direciona de como seria o rumo a ser seguido:

> 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

[38]MORAIS, José Luiz Bolzan de; MENEZES NETO, Elias Jacob de. **Marco Civil da Internet**: A insuficiência do marco civil da internet na proteção das comunicações privadas armazenadas e do fluxo de dados a partir do paradigma da surveillance. Organizadores: George Salomão e Ronaldo Lemos. São Paulo: Atlas, 2014, p. 425.

> 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[39].

Com o projeto de lei já nas casas Legislativas, ouve um *boom* que ajudou na aprovação mais rápida dessa lei. Instigada a aprovação pela comoção social e midiática advinda com a publicação de fotos íntimas da conhecida atriz brasileira Carolina Dieckmann.

A atriz foi *hackeada* e os invasores tiveram acesso a fotos e informações privadas, usando esse material como uma moeda de troca. O objetivo do cibercriminoso era de barganhar dinheiro da atriz em troca de não divulgar o material por ele adquirido. A atriz não cedeu a chantagem, em consequência suas fotos íntimas foram divulgadas, acarretando uma grande repercussão e um enorme constrangimento a vítima, pois, havia dentre o material adquirido pelo criminoso, fotos sensuais da atriz.

Em consequência dessa repercussão e da pressão popular em frete ao poder legislativo no dia 30 de novembro de 2012, foi sancionada e posta em vigor a Lei 12.735, ficando conhecida pelo mesmo nome da atriz “Lei Carolina Dieckmann”[40].

Prevendo a possibilidade de invasão o Estado subordinou a maneira de exercer o poder punitivo que lhe é devido, garantindo a prevenção dos princípios constitucionais antes citados, o objetivo central lei Carolina Dieckmann é a proteção dos dispositivos informáticos, quando esses dispositivos se encontrarem protegidos por programas específicos de segurança.

A existência de um mecanismo de segurança com a função de proteger os aparelhos eletrônicos, como antivírus, senhas e outras defesas digitais,detêm grande parte das invasões, contudo, quando esses dispositivos sofrem uma simples violação dessas defesas já configura crime, baseando-se no direito a privacidade.

Pedro Beretta afirma que embora a criação da lei tenha sucedido bem, à forma estabelecida foi equivocada, mesmo assim é um passo considerável para o combate ao cibercriminoso:

> [...] demonstrou, mesmo que de forma equivocada, a preocupação do Estado em tutelar diversas mudanças trazidas pela tecnologia da

[39]PINHEIRO, Patrícia Peck; HAIKAL, Victor Auilo. **A nova lei de crimes digitais**. 2013. Disponível em: www.pppadvogados.com.br/Publicacoes.aspx?v=1&nid=1432. Acesso em: 23 mar. 2019
[40]BRASIL.Lei Nº 12.737, de 30 de Novembro de 2012.**Lei Carolina Dieckmann.**Disponível em :http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 25 abr. 2018.

> informação, sendo de grande importância o reconhecimento de medidas para proteger os aspectos de liberdade individual do cidadão e também eventuais prejuízos de ordem material originários de uma “nova prática ilícita[41].

A lei que veio com a pretensão de ser complementar, alterando os diplomas legais já existentes:

> Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências[42].

O Marco Civil da Internet foi instituído no ordenamento jurídico em 2012/2014, influenciado pela crescente onda de ataques a sites oficiais do governo e de empresas públicas.

A busca pela proteção a informação foi o passo inicial para a criação do “Marco Civil da internet”, a partir dele, faz surgir a Lei nº 12.965/14, trazendo em seus artigos uma maior expansão das garantias individuais do usuário da Internet e os deveres e os direitos para o uso da internet no Brasil.

A lei para ser aprovada passou por longos debates durante a sua tramitação, a discussão girou em torno da liberdade, privacidade e a neutralidade da rede, destacando o papel de soberania pátria. Por ser a internet uma ferramenta onde o cidadão exerce sua função na sociedade manifestando sua liberdade, essa exposição faz com que a vida privada fosse violada e essa foi uma das preocupações do Estado ao criar a Lei 12.965/2014.

Não obstante, a lei estabeleceu regras para os provedores de internet, dentre as mais relevantes as que favorecem o direito à privacidade. A identidade do usuário deverá ser fornecida pelos provedores em casos específicos, mas, sempre por ordem judicial, visando a proteção individual e o direito à privacidade.

Após o Marco Civil da Internet, algumas questões foram trazidas com a Lei 12.965/2014, como a obrigação entre as operadoras provedoras de interneta

---

[41]BERETTA, Pedro. **Sem Meios Eficazes,** Lei Carolina Dieckmann até atrapalha. São Paulo: Dublê Editorial, 2014. Disponível em: https://www.conjur.com.br/2014-mai-10/pedro-beretta-meios-eficazes-lei-carolina-dieckmann-atrapalha. Acesso em: 10 mai. 2018.
[42]BRASIL, **Lei Nº 12.735,** de 30 de Novembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm**.** Acesso em: 28 jun. 2018.

guardaremos registros das conexões por um ano, e os registros de acesso por no mínimo seis meses:

> Art.13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de um ano, nos termos do regulamento. [...]Art. 15.O provedor de aplicações de internet constituídas na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de seis meses, nos termos do regulamento[43].

A Lei também trouxe benefícios aos provedores estabelecendo que a responsabilidade do conteúdo produzido seja do usuário, ressalvados os casos em que o conteúdo for em rede social, posto que,essas redes tem uma leva própria de serviço. Caso o conteúdo delituoso seja na rede social o provedor terá prazo para a retirada, se esse conteúdo não for retirado, o provedor responderá em qualquer esfera da justiça por eventuais danos causados pelo material publicado em suas páginas.

Grande é a divergência legislativa quando se trata de competência para julgamento dos crimes virtuais, visto que, no mundo informático o conceito de jurisdição perde um pouco a sua eficácia, pois a rede é um sistema mundial e os limites territoriais ficam perdidos nesse espaço sem fronteiras.

Os crimes plurilocais ocorrem quando a ação ou omissão acontecem em locais incertos, gerando assim uma série de conflitos de competência. O conflito existe porque o crime pode ser alcançado ao longo do território nacional dentre as fronteiras internacionais, gerando conflitos de competência trasfronteiriça[44].

A doutrina brasileira pensando numa solução para dirimir o conflito de competência usou a teoria mista, ou teoria da ubiquidade. Ficando definida a competência pelo local da infração, onde ocorreu a omissão ou a ação, em sua totalidade ou onde foi produzida maior parte dela conjuntamente onde produziu o resultado[45].

---

[43]BRASIL**, Lei Nº 12.965**, de 23 de Abril de 2014.Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 27 abr. 2018.
[44]PACHECO, Gisele Freitas – COSTA, Renato Lopes. **Crimes Virtuais e a Legislação Penal Brasileira.** Disponível em : http://fadipa.educacao.ws/ojs-2.3.3-3/index.php/cjuridicas/article/viewFile/269/pdf. Acesso em: 12 set. 2018.
[45]SILVA. Patrícia Santos da. **Direito e Crime Cibernético**: análise da competência em razão do lugar no julgamento de ações penais [recurso eletrônico] . Brasília, Ed. Vestnik, 2015. sn.

A norma adotada no Código Penal no seu Artigo 6° usa como base o princípio da territorialidade, da proteção, da justiça universal, da nacionalidade ativa e o da representação.

Para Eugênio Pacelli, dentro do ambiente nacional não deveria haver conflito, pois, a jurisdição é una:

> Como atividade e expressão do poder público, afirma-se que a jurisdição é una, no sentido de se tratar de intervenção do Estado junto aos jurisdicionados, para fins de atuação no direito ao caso concreto e, mais particularmente, nos que nos interessa de perto, ao caso ou questão penal[46].

É necessário, que as empresas armazenem essa gama de informações, por questões técnicas e gerenciais ou por norma legal as quais estão submetidas. Em diversos países o armazenamento de conteúdo produzido na internet é realizado seguindo o aspecto fiscal e econômico. Por razões de segurança esses servidores se espalham replicando seu conteúdo em vários cantos do globo e suas informações são fracionadas para depois serem armazenadas, preservando o conteúdo de possíveis ataques de criminosos.

Segundo La Chapelle e Fehlinger os possíveis critérios aventados para definir qual a lei aplicável na obtenção de dados digitais são:

> 1-a lei do local em que está o usuário, do qual se pretende obter os dados;
> 2- a lei do local onde estão os servidores que armazenam os dados;
> 3-. a lei do local de incorporação da empresa que presta o serviço;
> 4-a lei do local dos registradores de onde o domínio foi registrado.Todas as possíveis soluções apresentam dificuldades e podem conflitar com as regras de aplicação da lei penal de cada país (tradução nossa)[47].

As empresas provedoras ao assumirem que são detentoras do fornecimento dos dados digitais serão responsabilizadas subsidiariamente, para que, numa eventual solicitação judicial, tenha como fornece todas as opções mencionadas a cima.

Caso essa empresa provedora não atue para a disponibilização do conteúdo que auxilie a investigação, após receber a notificação judicial,surgirá a

---

[46]OLIVEIRA, Eugênio Pacelli de. **Curso de processo Penal**. 13. ed. Rio de Janeiro: Lummen Juris, 2010, p. 204.

[47]LA CHAPELLE, Bertrand; FEHLINGER, Paul. **Jurisdiction on the internet:** from legal arms race to transnational cooperation. Internet & Jurisdiction paper. Abr. 2016. Disponível em: https://www.internetjurisdiction.net/uploads/pdfs/Papers/IJ-Paper-Jurisdiction-on-the-Internet-PDF.pdf. Acesso: 06 jan. 2019.

responsabilidade subsidiária sobre esse fato, devendo retirar o conteúdo desde a sua notificação.

Posto as condições da responsabilidade dos provedores, deve analisar qual lei será aplicada. Deverá o juiz esclarecer fato danoso, direcionando qual medida será aplicada.

Apresentados os conceitos elementares à compreensão das particularidades da tipificação das condutas cibercriminosas, apontaremos as repercussões dessas particularidades no processo penal, isto é, no âmbito de investigação e da instrução de processos que envolvam cibercrimes. Para tanto, abordaremos no capítulo seguinte, os problemas particulares da produção da prova no Brasil e, em seguida, mais especificamente, as dificuldades da investigação nos crimes virtuais.

3 PROVA

A Prova é o instrumento pelo qual se tenta estabelecer a verdade de uma alegação ou de um fato, portanto cada fato existente no processo terá que ser comprovado. A lista de crimes teve um aumento considerável, contudo, não basta apenas a inclusão de novos tipos penais, uma vez que outras inovações foram trazidas com o surgimento desses crimes como àquelas relacionadas à investigação probatória[48].

Neste capítulo esboçaremos questões relativas as provas, aos aspectos gerais, ao objeto, características e meios das provas. Não tendo a pretensão de exaurir toda Teoria da Prova, mas, levantar alguns pontos a fim de compreender como as provas se comporta dentro do universo dos Crimes Virtuais.

3.1 Panorama Geral da Prova

O conceito de prova não é derivado do Direito, tem referência no pensamento científico de maneira geral. Aparecendo no Direito Processual como forma de traduzir os meios pelos quais o Estado/juiz e as partes se dispõem demonstrar sua pretensão em juízo, como também, para que a autoridade judiciária competente possa fundamentar sua decisão, tanto para a condenação de sujeitos ou para sua absolvição.

Deste modo, o conceito de provas pode ser adotado como a atividade designada para a colheita de elementos, que esclarecerão os pontos controversos de uma demanda judicial e formarão a convicção do julgador[49].

No Processo Penal, o objetivo das partes é convencer o julgador que os fatos narrados têm veracidade, as partes trazem para os autos um conjunto de material probatório destinados a contar uma história e provar a inocorrência ou ocorrência de um fato, portanto, a prova, é todo o elemento ou meio destinado ao convencimento do juiz dentro do processo.

Advinda da palavra latim *probation,*e do verbo *probare*, tem por significado reconhecer, persuadir, demonstrar ou examinar, sendo assim, a prova traz ao

[48]PINHEIRO, Patrícia Peck. **Direito Digital**. São Paulo: Editora Saraiva, 2013, p. 308.
[49]CINTRA, Antônio Carlos de Araújo; GRINOVER, Ada Pellegrini; DINAMARCO, Cândido Rangel. **Teoria Geral do Processo.** São Paulo: Malheiros Editores, 2010, p. 351.

processo todos os elementos que possam levar ao conhecimento de alguém a ocorrência de um fato.

Para Marinoni e Mitidiero, poderíamos definir a prova como “meio retórico, regulado pela legislação, destinado a convencer o Estado da validade de proposições controversas no processo, dentro de parâmetros fixados pelo direito e de critérios racionais”[50]

Gomes Filho enfatiza que: “Só a prova cabal do fato criminoso é capaz de superar a presunção de inocência do acusado, que representa a maior garantia do cidadão contra o uso arbitrário do poder punitivo”[51].Assim sendo, as provas é uma forma utilizada para garantir aos cidadãos Direitos em face do Estado.

> O processo penal deve construir a verdade judicial, sobre a qual, uma vez julgado a decisão final, incidirão os efeitos da coisa julgada, com todas as suas consequências, legais e constitucionais. O processo, portanto, produzirá uma certeza tipo jurídica, que pode ou não corresponder à verdade da realidade histórica, mas cuja pretensão é a de estabilização das situações eventualmente conflituosas que vem a ser o objeto da jurisdição penal [52].

O ato de provar constitui na busca pelo feito positivo, diante disso, as provas não pertencendo à apenas uma das partes. Todas as provas produzidas durante a investigação e processo serão efetivas para ao interesse jurisdicional, alocados positivamente pra apreciação do juiz, e assim,chegar a uma verdade. Em síntese, é a conformidade da noção ideológica com a realidade, não estando sempre atreladas à certeza.

O objeto da prova recai sobre os fatos relevantes, notórios, pertinentes, impossíveis e aqueles contidos em presunção legal absoluta. A reconstrução da verdade dos fatos, ocorridos efetivamente no espaço e tempo, é uma tarefa árdua para chegar à reconstrução real dos fatos ocorridos, os quais deram ensejo ao processo. Neste sentido Oliveira Pacelli clareia o objetivo da prova dentro do processo penal, quando diz:

---

[50]MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Código de processo civil comentado**. São Paulo: RT, 2011. 3ª ed. p. 334

[51]GOMES FILHO, Antônio Magalhães, Notas sobre a terminologia da prova.*In:* YARSHELL, Flávio Luiz; MORAES, Maurício Zanoide (Orgs.). **Estudos em homenagem à Professora Ada Pelegrine Grinover**. São Paulo: DPJ, 2005, p. 56.

[52]OLIVEIRA, Eugênio Pacelli de.**Curso de processo Penal**. 13. ed. Rio de Janeiro: Lummen Juris, 2010, p. 304.

> O processo penal deve construir a verdade judicial, sobre a qual, uma vez julgado a decisão final, incidirão os efeitos da coisa julgada, com todas as suas consequências, legais e constitucionais. O processo, portanto, produzirá uma certeza tipo jurídica, que pode ou não corresponder à verdade da realidade histórica, mas cuja pretensão é a de estabilização das situações eventualmente conflituosas que vem a ser o objeto da jurisdição penal [53].

Sendo assim, para que o juiz chegue ao final de um processo é necessário relacionar juridicamente os atos praticados e o recolhimento probatório, verificando que toda ação jurisdicional esteja conectas. O ato desde a instrução criminal até a instrução probatória levadas em juízo pelas partes devem estar fundidas.

Diante das diversas etapas da descoberta de um crime, as provas colhidas na investigação exercem um protagonismo quando tratamos dos cibercrimes. Na primeira fase (fase da investigação) levantam-se as provas periciais ou provas técnicas, provas que não se sujeitam ao contraditório, pois, serão avaliadas posteriormente no processo. São de suma importância para a descoberta do fato e do criminoso e se mostram indispensáveis dentro da investigação de crimes virtuais.

Essas provas colhidas na fase pré-processual direcionam o rumo do processo. Nas palavras Aury Lopes Jr. “O esgotamento da eficácia probatória com a admissão da acusação, serve para justificar medidas cautelares na faze pré-processual e para justificar o processo ou o não processo”[54]. Mas mesmo sendo colhidas na fase pré-processual, essas provas ficarão sempre atreladas ao processo.

Nucci aplica três sentidos ao ato de provar; o começo, o meio e o fim:

> 1º - Começo, o ato de provar é o processo pelo qual se verifica a exatidão ou a verdade do fato alegado pela parte no processo, 2º- Meio de provar, trata-se do instrumento pelo qual se demonstra a verdade de algo, 3º- Fim, resultado da ação de provar, é o produto extraído da análise dos instrumentos de provas oferecidos, demonstrando a verdade de um fato[55]

Ao longo da história o tema construção da verdade foi um embate para o direito, e é assim até os dias de hoje, e ainda, mais desafiador, pelo avanço tecnológico. Os meios e métodos utilizados para chegar obtenção da verdade são

---

[53]OLIVEIRA, Eugênio Pacelli de.**Curso de processo Penal**. 13. ed. Rio de Janeiro: Lummen Juris, 2010, p. 304.
[54]LOPES JR, Aury. **Direito Processual Penal e Sua Conformidade Constitucional.** 8.ed.Lumen Juris. Rio de Janeiro, 2011, p. 306.
[55]NUCCI, Guilherme de Souza, **O Valor da Confissão como meio de Prova no Processo Penal**, 2. ed., rev. E atual. São Paulo: Revista dos Tribunais, 1999, p. 350.

os mais variados, isto é, que o conceito não é apenas um, quando se trata de definir o que é prova. Para Oliveira Pacelli provar é:

> A reconstrução dos fatos investigados no processo, buscando a maior coincidência possível com a realidade histórica, isto é, com a verdade dos fatos, tal como efetivamente ocorrido no espaço e no tempo. A tarefa, portanto, é das mais difíceis, quando não impossível: a reconstrução da verdade[56].

Na antiguidade, os costumes eram a base para dirimir os conflitos, os âmbitos Filosóficos e Religiosos ditavam as regras. Variados meios de se chegar a verdade foram utilizados durantes os séculos, passando desde as ordálias encontradas no ano de 2.100 a.C.[57], Na antiguidade, os costumes eram a base para dirimir os conflitos, os âmbitos Filosóficos e Religiosos ditavam as regras. Variados meios de se chegar a verdade foram utilizados durantes os séculos, passando desde as ordálias encontradas no ano o Código Ur-Nammu, 200 a.C.[58]e o de Código de Hamurabi, 1772 a.C[59].

Roma, abriu um precedente jurídico no que diz respeito as provas, passando a levar à apreciação jurídica para as praças, fazendo com que o povo se pronunciasse sobre o fato emitindo opiniões, e por fim, tomasse mas decisões. Não podemos dizer que era de fato uma apreciação jurídica de provas, mas, o povo participava ativamente da resolução dos problemas sócio-criminais.

No Brasil, adotamos o sistema do livre convencimento motivado, onde a autoridade judicial é livre para decidir e apreciar as provas, fazendo-o sempre de forma fundamentada, dentro dos exatos termos prescritos no art. 93, IX da Constituição Federal com a redação dada pela Emenda Constitucional nº 45, de 2004.

> Todos os julgamentos dos órgãos do Poder Judiciário serão públicas e fundamentadas todas as decisões, sob pena de nulidade, podendo a lei limitar a presença, em determinados atos, às próprias partes e a seus advogados, ou somente a estes, em casos nos quais a preservação do

---

[56]OLIVEIRA, Eugênio Pacellide.**Curso de processo Penal**. 13. ed. Rio de Janeiro: Lummen Juris, 2010, p. 315.
[57]HISTÓRIAZONE, Jul 14, 2016, **As ordálias da Idade Média, ou "o juízo de Deus.** Disponível em: https://historiazine.com/as-ordalias-da-idade-media-d090cbac4831. Acesso em 28 mar. 2019
[58]MANUSRTI- **Código de Manu** (200 A.C. e 200 D.C.). Disponível em: http://www.ufra.edu.br/legislacao/CODIGO%20DE%20MANU.pdf. Acesso em: 29 mar. 2018.
[59]KERSTEN, Vinicius Mendez. Ano 2017. **O Código de Hamurabi através de uma visão humanitária.** Disponível em: http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=4113. Acesso em: 28 mar. 2018.

> direito à intimidade do interessado no sigilo não prejudique o interesse público à informação[60].

Ainda sobre o sistema utilizado no Brasil, Ada Pelegrini ensina que:

> [...] o princípio da verdade real, que foi o mito de um processo penal voltado para a liberdade absoluta do juiz e para a utilização de poderes ilimitados na busca da prova, significa hoje simplesmente a tendência a uma certeza próxima da verdade judicial: uma verdade subtraída à exclusiva influência das partes pelos poderes instrutórios do juiz e uma verdade ética, processual e constitucionalmente válida. Isso para os dois tipos de processo, penal e não penal. E ainda, agora exclusivamente para o processo penal tradicional, indica uma verdade a ser pesquisada mesmo quando os fatos forem incontroversos, com a finalidade de o juiz aplicar a norma de direito material aos fatos realmente ocorridos, para poder pacificar com a justiça[61].

Ao longo do processo algumas provas serão descartadas, dependerá tão somente da relevância que essa prova trará ao processo. Sendo examinadas apenas provas necessárias.

A prova cumpre seu papel no processo quando auxilia o juiz a tomar sua decisão, por isso, todas as provas têm um valor e terão o exato momento para exercer a função de narrar os fatos para o magistrado.

Quando se trata de valoração das provas Marina Gascón Anellán conceitua de maneira clara quando diz:

> A valoração das provas é o juízo de aceitabilidade dos resultados produzidos pelos meios de prova. Consiste, especificamente, na verificação dos enunciados fáticos introduzidos no processo por intermédio dos meios de prova, assim, como no reconhecimento dos mesmos por um determinado valor ou peso na formação da convicção do julgador sobre os fatos que são considerados[62].

Não há hierarquia nas provas, por conta da sua Natureza Jurídica, isto é, a essência dessa natureza é a subjetividade, por conseguinte, a valoração da prova deve conceber-se como uma atividade racional, consistente na eleição da hipótese mais provável entre as diversas reconstruções possíveis dos fatos[63].

---

[60]BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 29 mar. 2018.
[61]GRINOVER, Ada Pellegrini. **A Iniciativa Instrutória do Juiz no Processo** penal acusatório. Brasília, Revista Jurídica Consulex, nº. 169, p.33-36, Out. 2006.
[62]ABELLÁN, Marina Gascón. **Los hechosenel derecho:** bases argumentales de la prueba. Madrid: Marcial Pons, 1999, p. 157. (tradução nossa).
[63]ABELLÁN, Marina Gascón op. cit., p. 161. (tradução nossa).

O ônus da Prova, portanto, recai sobre a pessoa a que trouxe a prova aos autos do processo, incidido a obrigação de comprovar a veracidade quem as trouxe para o processo.

Significa dizer que, as provas têm valor para o sujeito que as revelou no processo, e esse sujeito, é quem deverá sustentá-las em juízo, independente de qual pólo da ação o sujeito se encontre.

Para Pietro Perlingieri; “O ônus é a situação passiva na qual o titular deve comportar-se não no interesse de outrem, mas a si próprio. O ônus é definido [...] como oblíquo potestativo, no sentido de que o seu titular pode realizá-lo ou não”[64].

As provas deverão estar atrelas ao processo, preservando o contraditório diante dela. O ônus da prova é o encargo que as partes têm de provar os fatos que alegam. Dentro dos termos do art. 156 do Código de Processo Penal, o ônus da prova incumbe a quem fizer a alegação.

3.2 Meios de Prova

São considerados meios de provas, tudo que podem ser utilizados direta ou indiretamente a fim de comprovar os fatos alegados no processo.

Nas palavras de Paulo Rangel, meios de provas “são todos aqueles que o juiz, direta ou indiretamente, utiliza para conhecer da verdade dos fatos, estejam eles previstos em lei ou não”[65]. A não previsibilidade legal está relacionada ao princípio da verdade real, que determina a não há limitação de prova, isto é, permitem meios não previstos em lei, dede que, esses meios não afrontem o ordenamento jurídico e não sejam ilegítimos e ilegais.

Todo o processo tem atrelado em si a sua busca pela verdade, mas, para que isso aconteça, utiliza de caminhos nos quais suas convicções vão tomando forma e clareza, para que no final do processo, venha a proferir uma decisão perto da verdade e justa. Como o ordenamento jurídico não pode haver contradição, extraímos o conceito do Código de Processo Civil:

---

[64]PERLINGIERI, Pietro. **O Direito Civil na Legalidade Constitucional.** Trad. Maria Cristina de Cicco. Rio de Janeiro. Ed. Renovar, 2008, p. 698

[65]RANGEL, Paulo. **Direito Processual Penal**. Rio de Janeiro. Lumen Juris, 2003, p. 417.

> "Art. 369 As partes têm 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"[66].

Os meios de provas são vastos, podendo ser usados em momentos oportunos no processo, o rol descrito em todo Código de Processo Penal é meramente exemplificativo, portanto, a diversidade é considerável.

Os mais relevantes meios de prova usados para solucionar um crime virtual são:

Interrogatório, um dos meios de prova mais utilizados no mundo equivale no ato por meio do qual o magistrado ouve o acusado, colhendo informações sobre a pessoa do acusado e sobre os fatos, as perguntas realizadas, trilham um caminho para chegar ao elemento de convicção do julgador.

Tendo também, por característica à autodefesa, isto é, o acusado poderá alegar exatamente o que lhe favorecer e a qualquer tempo do processo. O interrogatório poderá ser realizado a pedido do acusado, do juiz ou do acusador, mas, somente o juiz poderá formular perguntas e questionar o acusado dos fatos, caso houver mais de um acusado, serão ouvidos separadamente [67].

Aranha descore acerca do interrogatório da seguinte forma:

> Admitindo-se como meio de Prova o juiz perguntará ao acusado livremente, respeitados apenas os princípios gerais ligados à colheita de provas [...] na hipótese de ser entendido como meio de defesa, o acusado caberá a narrativa, funcionando como uma oportunidade para dar a sua versão e exculpar-se, se for o caso [68].

A Confissão é o ato processual direcionado ao acusado, onde ao ser questionado à cerca dos fatos a ele imputados, terá a oportunidade de falar acerca do ocorrido, negando ou afirmando acerca dos fatos. Também pelo Direito Constitucional, o acusado poderá ficar em silêncio, e esse silêncio não pode ser interpretado por uma aceitação tácita, portanto, não poderá trazer prejuízo ao acusado.

---

[66]BRASIL, **Lei Nº 13.105**, de 16 de Março de 2015**.**
Disponível em:http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.ht. Acesso em: 17 abr. 2018.
[67]ARANHA, Adalberto José Q.T. Camargo. **Da Prova no Processo Penal**. 7. ed. São Paulo: Saraiva, 2006, p. 98.
[68]ARANHA, op. cit., p. 112.

A confissão poderá ser exercida no interrogatório ou a qualquer tempo do processo. Aranha conceitua que “a confissão é a declaração de voluntária, feita por um imputável, a respeito de um fato pessoal e próprio, desfavorável e suscetível de renúncia[69]. Para Távora e Antonni “confessar é reconhecer a autoria da imputação ou dos fatos, objeto da investigação preliminar por aquele que está no pólo passivo da persecução penal”[70].

A confissão deve de ser real e espontânea, como apresenta Nucci:

> A confissão deve ser um ato voluntário, produzido livremente pelo agente, sem nenhuma espécie de coação, expresso, ou seja, manifestado sem dúvida nos autos e pessoal, não sendo possível a confissão no processo penal feita por mandatário, o que atentaria contra a segurança do princípio da presunção de inocência[71].

A confissão será validada pelo juiz, se houver concordância ao ser devidamente confrontada com outras provas apresentadas no processo, valorada igualmente a qualquer outra prova apresentada.

Uma particularidade desse meio de prova é que havendo co-réus, a confissão exercida por um ou mais de um acusado, não estenderá seus efeitos até os outros, mas, diante de uma confissão, poderá se entender como validação para defesa de terceiros. Levando em consideração que o processo penal a individualização do sujeito é necessária para a aplicação da pena.

No sistema brasileiro, o meio de prova mais comum utilizados pelo judiciário é a prova Testemunhal, por não haver requisito de especificidade, isto é, qualquer pessoa poderá exercer o papel de testemunha. O Código de Processo Penal no Art. 102 reafirma isso, "Toda pessoa poderá ser testemunha”[72].Mas, em caso excepcionais essa testemunha poderá renunciar, nos termos que a lei determina em um rol taxativo no Art. 206 do Código Penal:

> Testemunha não poderá eximir-se da obrigação de depor. Poderão, entretanto, recusar-se a fazê-lo o ascendente ou descendente, o afim em

---

[69]ARANHA, Adalberto José Q.T. Camargo. **Da Prova no Processo Penal**. 7. ed. São Paulo: Saraiva, 2006, p.76.
[70]TÁVORA, Nestor. ANTONNI, Rosmar. **Curso de Direito Processual Penal**. 3. ed. Salvador: Jus Podivm, 2009, p. 359.
[71]NUCCI, Guilherme de Souza, **O Valor da Confissão como meio de Prova no Processo Penal**, 2. ed., rev. E atual. São Paulo: Revista dos Tribunais, 2011, p. 136.
[72]BRASIL. Decreto-Lei Nº 3.689, 3 de outrubro de 1941. **Código de Processo Penal**, 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm. Acesso em: 30 mar. 2018.

> linha reta, o cônjuge, ainda que desquitado, o irmão e o pai, a mãe, ou o filho adotivo do acusado, salvo quando não for possível, por outro modo, obtiver-se ou integrar-se a prova do fato e de suas circunstâncias[73].

A definição do professor Adalberto Aranha acerca do que é uma testemunha, é esclarecedora, ele diz que: "Testemunha é todo homem, estranho ao feito e equidistante às partes, capaz de depor, chamado ao processo para falar sobre o fato caído sob seus sentidos e relativos ao objeto do litígio[74]. Existe a testemunha direta, que é aquela que presenciou o fato, ou indireta, aquela que ouviu sobre o fato. O número de testemunhas depende do procedimento adotado, podendo chegar a alguns casos até o número de oito.

Concordamos com José de Aquino, quando ele afirma não restar dúvida que:

> O testemunho, no processo penal, é o centro das investigações, influindo sobremaneira na *opinio delicti* do representante do Ministério Público e na convicção do julgador. [...] quanto mais consentâneo com a realidade for o testemunho, mais provável será que o agente do Poder Judiciário julgue o caso que se encontra sob sua apreciação, como se ele próprio tivesse testemunhado o fato[75].

Por esse motivo que as provas testemunhais são tão utilizadas, pela facilidade de ser conseguida, e pelo grau de esclarecimento que poderá trazer ao julgador.

Outro meio de prova que traz testemunhas ao processo, mas não é o meio de prova testemunhal, é o Reconhecimento de Pessoas e das Coisas. Esse meio de prova tem como objetivo confirmar a identidade de algo (objeto) ou de uma pessoa, e está vinculado ao fato criminoso. É visto como um confronto direto com a memória da testemunha que presenciou o fato narrado no processo.

Aury Lopes Jr. define o reconhecimento como: "Um ato através do qual alguém é levado a analisar alguma pessoa ou coisa e recordando o que havia percebido em um determinado contexto, compara as duas experiências"[76].

A valoração desse reconhecimento é formalmente preestabelecida, e está sujeita, ao confronto com as outras provas. O objetivo desse meio de prova é levar a

---

[73]BRASIL. Decreto-Lei Nº 3.689, 3 de outrubro de 1941. **Código de Processo Penal**, 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm. Acesso em: 30 mar. 2018.
[74]ARANHA, Adalberto José Q.T. Camargo. **Da Prova no Processo Penal**. 7. ed. São Paulo: Saraiva, 2006,p. 103.
[75]AQUINO, José Carlos G. Xavier de. **A prova testemunhal no processo penal brasileiro**. 4.ed. São Paulo: Juarez de Oliveira, 2002, p.15.
[76]LOPES JR., Aury. **Direito Processual Penal**. 10. ed. São Paulo: Saraiva, 2013, p.76.

uma verdade convincente para o julgador, portanto, o juiz aplica a essa testemunha o confronto, com pessoas semelhantes fisicamente, reconhecimento através de fotografias (mesmo não estando no CPP), e o reconhecimento de objetos como roupas, armas.

Um dos meios de provas indispensável dentro do processo penal, e totalmente cabal nos crimes virtuais, é a prova Pericial. Equivale dizer que a prova pericial é a forma de trazer ao processo evidências materiais, isto é, através delas que o juiz confirma a materialidade dos fatos.

Para Aranha a natureza jurídica da perícia é de “um meio instrumental, técnico-opinativo e alicerçado da sentença”[77]

A prova pericial tem por característica a tangibilidade, por essa razão a sua coleta necessitará de peritos, ou técnicos especializados, para que assim, as informações contidas cheguem ao processo intactas.

Poderá ser realizada na fase pré-processual (inquérito), como também, nas fases posteriores (processo). Os laudos periciais poderão ser questionados, caso seja, a vontade das partes, por esse motivo a coleta do material probatório deve ser rigorosa, assim sendo, não deixará dúvidas no julgador.

Documentos também são admitidos como meios de prova material, chegando ao processo de forma escrita, por meios eletrônicos, papéis públicos ou particulares, pinturas, desenhos, fotografias, vídeos, gravações fonográficas entre outros.

Os documentos como meio de prova, deverão ser trazidos ao processo por uma vontade voluntária, que seja relevante e elucidativa para o processo. Esses documentos deverão ser confrontados com as outras provas e checados amplamente, a fim de garantir sua validade para que só assim, produzam efeitos de prova.

Outro meio de prova utilizado dentro do no nosso ordenamento jurídico, são os Indícios, sendo constituídos numa reunião e interpretações em face de uma série de fatos e circunstâncias relativas ao injusto determinado. Muito divergente em nossa doutrina, pois, para alguns não seriam exatamente um meio de prova, por não se sustentarem isoladamente no processo, isto é, não teriam um valor em si mesmo, só corroboraria com outro meio de prova.

---

[77] ARANHA, Adalberto José Q.T. Camargo. **Da Prova no Processo Penal**. 7. ed. São Paulo: Saraiva, 2006,p. 111.

Os indícios, apesar dessa divergência estão sendo recebido pelos tribunais e obtendo a mesma valoração como qualquer outro meio de prova, sendo sustentadas em muitos casos em si mesmo, pelos seus efeitos no processo sendo igual a qualquer outro meio de prova.

A doutrina é convergente e atribuem aos indícios um caráter de prova semiplena, parcial ou indireta, dedutiva, portanto, nesse aspecto deveria o juiz ter cautela nas provas indiciárias, Aury Lopes Jr. tem essa mesma interpretação quando diz que: "Não se pode confundir provas com indícios, ainda que toda a prova seja um indício do que ocorreu" [78].

A natureza da prova indiciária é fruto da lógica, sua relação com uma determinada norma de experiência dedutiva e indutiva, uma presunção de certeza do fato ocorrido.

Em todo caso, a prova indiciária tem valia quando é confrontada com as demais provas, não sendo por si só objeto de condenação, pois o dever de comprovar que o fato ocorreu o é de quem acusa, e a certeza de que o fato aconteceu advêm das provas que são apresentadas no processo como um todo, como descrita de maneira bastante explícita no Código de Processo Penal no Título VII. Art. 155 a 250 "[...] enfim, tudo aquilo que o juiz utiliza para alcançar um fim é considerado meio de prova"[79].

A prova indiciária tem um valor diferenciando em detrimento dos crimes virtuais, visto que, elas darão um rumo à investigação probatória. O grau de dificuldade de comprovar a autoria nos crimes cometidos virtualmente faz com que os indícios, tenham um papel crucial no processo.

Podemos considerar também, que não se pode confundir meio de prova com fontes de prova, pois, as fontes são interligadas com pessoas ou coisas, acerca das quais, sendo basicamente tudo que indica algum fato ou afirmação útil, no qual, as comprovações sejam necessárias para a confirmação da verdade, como uma peça acusatória (denuncia ou queixa).

---

[78]LOPES JUNIOR, Aury, **Direito Processual Penal**. 10. ed. São Paulo: Saraiva. 2013, p.134.
[79]BRASIL. Decreto-Lei Nº 2.848, de 7 de Dezembro de 1940. **Código Penal**, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em: 15 fev. 2018.

3.3 O objeto, A Classificação e o Sistema de Apreciação das Provas.

O objeto da prova é qualquer fato que influencie no processo. Segundo Nestor Távora e Rosmar Rodrigues, “o objeto da prova consiste nos fatos que fundamentarão a ação e a defesa capazes de influenciar na decisão do juiz, na responsabilidade penal e na fixação da pena, necessitando, portanto, de adequada comprovação em juízo”[80], isto é, são circunstâncias baseadas nos fatos, pessoas, documentos, lugares e objetos.

Tudo que leve a reconstrução e esclareça a história relatada pode ser considerado objeto da prova, colaborando para que o julgador exerça seu juízo de valor, checando os fatos narrados em conformidade com todas as provas trazidas ao processo, certificando assim, a veracidade de cada uma delas.

Para Tourinho Filho o “Objeto de prova é o *thema probandum*, o fato a ser provado. [...] se usarmos o termo “objeto de prova” no sentido daquilo que devem ser provados, então, todos os fatos sobre os quais versa a lide são objetos de prova[81].

Paulo Rangel faz uma diferença entre o objeto DE prova e o objeto DA prova, vejamos:

> Há diferença entre objeto **da** prova e objeto **de** prova. O objeto de prova significa todos os fatos ou coisas que necessitam da comprovação de sua veridicidade. Na ocorrência de um processo, tanto o autor quanto o réu apresentam argumentos favoráveis a eles mesmos, assim como acontecimentos que demonstrem a veracidade de suas alegações. Ocorrendo isso, os mesmos acabam por delimitar o objeto da prova, devendo o julgador ater-se à somente estes fatos[82].

O objeto é a base que será levada ao juízo para comprovar a veracidade do direito ou o fato, ao **Objeto, ao Sujeito e Forma**, existe a corrente minoritária traz consigo o elemento de **valor**, que seria o grau de certeza que essa prova será usada, seriam as provas necessárias e cruciais que o julgador utiliza para valorar e ter a certeza que fato ficou esclarecido, auxiliando na sua decisão.

Quanto aos **sujeitos** da prova é a coisa ou a pessoa de quem ou de onde emana a prova, afirmando que se quer provar, sem a necessidade de provar os

---

[80]TÁVORA, Nestor. ANTONNI, Rosmar. **Curso de Direito Processual Penal**. 3. ed. Salvador: Jus Podivm, 2009, p. 244.
[81]TOURINHO FILHO, Fernando da Costa. **Processo Penal**. São Paulo: 2005, p. 187.
[82]RANGEL, Paulo. **Direito Processual Penal**. 20. ed. São Paulo: Atlas, 2012, p.381.

fatos notórios de conhecimento público. Segundo Heráclito Mossim, “o fato notório é aquele de existência vulgarizada, indicando-se uma verdade irretorquível que deve ser aceita sem discrepância”[83].

Os sujeitos da prova, portanto, são os quais interferem no processo penal consoante com as peculiaridades que lhes são conferidas por lei, contribuindo para o alcance das finalidades do processo de lograr a aplicação justa.

O **Objeto** da prova é o fato a qual, se quer provar, podendo ser o objeto da prova direta ou indireta. Prova Direta está ligada imediatamente ao fato a ser provado, as provas Indiretas também chamadas de circunstanciais, dizem respeito a outro fato que, por sua vez, se liga ao fato a ser provado. São provas indiretas as presunções e indícios.

Por fim, a **Forma** da prova é a modalidade ou maneira pela qual a prova se apresenta em juízo. Diz-se material a prova consistente em qualquer materialidade que sirva de prova ao fato probando, é a atestação emanada da coisa.

O sujeito, a forma e o objeto auxiliam ao julgador tomar a sua decisão, porém, o Direito Penal deverá manter-se atualizado usado a tecnologia a seu favor, tal qual, o criminoso utiliza para cometer os cibercrimes[84].

O Processo Penal obedecendo às regras estabelecidas no Código Processual brasileiro usa o Sistema da Persuasão Racional ou do Livre Convencimento Motivado para solucionar os litígios.

Deste modo, o julgador terá liberdade para decidir e apreciar as provas, da maneira que lhe convier, tendo em vista que, não há critérios legais de fixação dos valores probatórios. Conforme exposto no Artigo 155 do Código de Processo Penal:

> O juiz formará sua convicção pela livre apreciação da prova produzida em contraditório judicial, não podendo fundamentar sua decisão exclusivamente nos elementos informativos colhidos na investigação, ressalvados as provas cautelares, não repetíveis e antecipadas[85].

No entanto, o processualista Aury Lopes Jr. adverte que:

---

[83]MOSSIM, Heráclito Antônio. **Compêndio de Processo Penal**. São Paulo: Manole, 2010, p. 306.
[84]RANGEL, Paulo. **Direito Processual Penal**. 20. ed. São Paulo: Atlas, 2012, p. 382
[85]BRASIL. Decreto-Lei Nº 3.689, 3 de Outubro de 1941. **Código de Processo Penal**, 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm. Acesso em: 30 mar. 2018.

> O livre convencimento motivado,na verdade não é um sistema tão livre como se pensa, pois a liberdade não é plena, uma vez que a decisão judicial deve estar consubstanciada na prova produzida, vedando-se o decisionismo, ou seja, não admite-se em um processo penal democrático, como é o nosso, que o juiz julgue conforme a sua consciência, dizendo qualquer coisa sobre qualquer coisa[86] .

Outros sistemas existem, mas, não foram adotados pelo Código de Processo Penal, mas são utilizados em alguns casos.

O Sistema da Prova Tarifada ou Da Verdade Legal ou Formal, onde a lei atribui o valor a cada prova, cabendo ao juiz simplesmente obedecer ao mandamento legal. Não é adotado no nosso ordenamento jurídico, salvo em algumas hipóteses em que a lei determina: 1- Prova quanto ao estado das pessoas, exigindo a apresentação de documento hábil a fim de que seja demonstrado o estado civil da pessoa; 2- Nos crimes que deixam vestígios será indispensável o exame de corpo de delito para que demonstre sua existência. Nos processos onde os crimes são virtuais esse sistema é de suma importância pela dificuldade na investigação da autoria.

O sistema da persuasão racional traz certa segurança ao processo, visto ser possível saber de antemão o valor de cada prova. Podemos dizer que não existe uma hierarquia entre as provas, é o julgador que decide livremente e de acordo com sua consciência.

Tendo o juiz uma liberdade comedida, isto é, a decisão não é absoluta, diante disso, deverá o juiz explicar e fundamentar quais foram as suas motivações, e como tomou cada decisão dentro do processo.

Paulo Rangel faz uma ressalva ao dizer que:

> Apesar do sistema da persuasão racional não estabelecer valor entre as provas, ou seja, apesar de não haver hierarquia entre as provas, o juiz deve fundamentar as suas decisões com base nas provas produzidas sobre o crivo do contraditório e do devido processo legal, não se aceitando a condenação de um indivíduo com base, única e exclusivamente, em elementos colhidos na fase de investigação, pois nessa fase (pré-processual) o contraditório é mitigado[87].

Os Princípios do sistema de provas também auxiliam o juiz na fundamentação da sua decisão.

---

[86]LOPES JUNIOR, Aury, **Direito Processual Penal**. 10. ed. São Paulo: Saraiva. 2013, p.278.
[87]RANGEL, Paulo. **Direito Processual Penal**. 20. ed. São Paulo: Atlas, 2012.p. 427.

De início citaremos o Princípio da Alta Responsabilidade das Partes, principio esse, que está diretamente relacionado ao ônus da prova. Entendendo que as partes do processo devem produzir provas e trazê-las em juízo como pressuposto das suas alegações, essas provas ficam diretamente correlacionadas com os fatos mencionados, e assim, responsabilizando o agente que as trouxe a comprovar a sua veracidade.

O Princípio da Aquisição ou da Comunhão das Provas, diz respeito que no processo penal cada parte fica incumbida de produzir as suas provas, uma vez produzidas estas provas passam a fazer parte do processo, portanto, compartilhada por ambas as partes. Não pertence as provas apenas aquele que as produziu, mas, ao processo, colocadas a favor do juízo para valoração, justificando a sentença e oferecendo igualdade as partes.

Um dos princípios norteadores do Direito garantido na Constituição brasileira é o Princípio da Audiência Contraditória, nesse princípio as provas trazidas ao processo devem ser bilaterais, respeitando as garantias individuais propostas na nossa Constituição acerca da inviolabilidade da defesa. Vejamos o que diz o Art 5° LV. CF/88 "Aos litigantes, em processo judicial ou administrativo, e aos acusados em geral são assegurados o contraditório e ampla defesa com os meios e recursos a ela inerentes" [88].

Cabe destacar que, se a parte contraria não estiver ciente ou não obtiver oportunidade de se manifestar da prova apresentada, poderá acarretar nulidade, neste sentido Compaired e Santagati expressam que: "O princípio compreende necessariamente para comprovar um direito que dá a oportunidade da parte contrária se defender da prova oferecida, podendo acarretar nulidade" [89](tradução nossa).

Um princípio discutido pela doutrina é o Princípio do Livre Convencimento Motivado, pela importância dele no processo, visto que, ele trata do poder que é dado pelo Estado ao juiz, carregando sobre si a tarefa de valorar cada prova apresentada.

Estado, porém, não fixa em lei qual o valor de cada prova, ficando essa tarefa concentrada, na consciência intrinca do julgador, isto não significa que o juiz pode

[88]BRASIL. **Constituição do Brasil**,1998 Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 29 mar. 2019.
[89]COMPAIRED, Carlos Roman, SANTAGATI, Claudio Jesús. **Manual de Derecho Procesal Penal**. Buenos Aires: Juridicas, 2010, p.65.

dar qualquer sentença, assim, pelo raciocínio lógico, tendo suas convicções atreladas às provas apresentadas.

Neste sentido Compaired e Santagati conceituam que: “O processo tem um desenvolvimento concentrado, contraditório e oral, e a percepção direta das constantes e argumentações e a valorização correlativa geram o convencimento que leva à decisão” [90](tradução nossa).

Tendo em mãos os meios e princípios que norteiam o Direito, o juiz exercendo o papel do Estado, estará pronto para dar a sua sentença, seguindo o sistema de provas brasileiro apresentado acima.

Não obstante, existem alguns limites a serem seguidos em face do sistema de apreciação de provas, garantias para que as provas sejam imaculadas, e assim fluam sem contradições alcançando o papel de justiça.

Isto posto, é assertivo dizer que o processo não poderá usufruir de prova **Ilícita** e **Ilegítima,** mantendo os princípios legais estabelecidos no nosso ordenamento.

A Constituição Federal por meio de seu Art. 5º, LVI, deixa explicito que "são inadmissíveis, no processo, as provas obtidas por meios ilícitos"[91]. Como forma de regular a obtenção de provas, e de preservar o devido processo legal como também, uma proteção aos direitos fundamentais.

A prova ilícita está vinculada a maneira que foi obtida, isto é, o meio usado para seu recolhimento que incidirá na ilicitude. Não é admitida no processo, pois, ofende o direito material, retirando as garantias previamente estabelecidas no ordenamento jurídico.

A ilicitude da prova é caracterizada na maneira que foram obtidas, negligenciando as obrigações aos direitos e princípios descritos na norma jurídica, portanto, viola o Direito material no momento da coleta.

Dinamarco faz uso de uma bela definição quando diz que:

> Provas ilícitas são as demonstrações de fatos obtidas por modos contrários ao direito, quer no tocante às fontes de prova, quer quanto aos meios probatórios. A prova será ilícita – ou seja, antijurídica e, portanto, ineficaz a demonstração feita – quando o acesso à fonte probatória tiver sido obtido de modo ilegal ou quando a utilização da fonte se fizer por modos ilegais.

[90]COMPAIRED, Carlos Roman, SANTAGATI, Claudio Jesús. **Manual de Derecho Procesal Penal**. Buenos Aires: Juridicas, 2010. p.69.
[91]BRASIL. **Constituição do Brasil**,1998. Disponível em :http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 12 mar. 2019.

> Ilicitude da prova, portanto, é ilicitude na obtenção das fontes ou ilicitude na aplicação dos meios. No sistema do direito probatório, o veto às provas ilícitas constitui limitação ao direito à prova. No plano constitucional, ele é instrumento democrático de resguardo à liberdade e à intimidade das pessoas contra atos arbitrários ou maliciosos[92].

Documentos falsificados, grampos se autorização judicial, confissão por meio de tortura, são alguns exemplos de provas ilícitas. A prova que é obtida por meio ilícito automaticamente é nula, pois, a ilicitude é desde a sua origem.

Diferentes das provas ilícitas são as provas ilegítimas, caracterizada toda vez que o direito processual é violado. Ao curso do processo a prova que produzida de alguma maneira conflita com o regramento processual será considerada prova ilegítima, visto que as normas processuais são preestabelecidas.

Salienta-se que a falta de veracidade não é tão-somente porque a prova é falsa, viciada ou foram colhidas de maneira ilegal, mas, o conteúdo dessas provas que são ilegítimos, portanto, mesmo que essas informações sejam obtidas por meios legais, não cumpriram as formalidades previstas na norma.

Vejamos o conceito dado por Paulo Rangel:

> São irregulares (ilegítimas) as provas que, não obstante admitidas pela norma processual, foram colhidas com infringência das formalidades legais existentes. Quer-se dizer, embora a lei processual admita (não proibida) um determina o tipo de prova, ele exige, para a sua validade, o cumprimento de determinadas formalidades que não são cumpridas[93].

Pacificando o assunto sobre provas ilícitas e ilegítimas, existe um princípio ou teoria, fincada em nosso sistema jurídico que é o, Princípio do Fruto da Árvore Envenenada. Aduz a esse princípio que toda prova produzida em consequência do ilícito, estará também todo o conteúdo contaminado pela ilicitude.

Para conservar a segurança jurídica, o sistema de provas não pode dar brecha a dúvida, assim sendo, todas as derivações de uma prova considerada ilícita, será por analogia contaminada com a ilicitude inicial, por consequência não será acolhida em juízo.

Também chamado de prova ilícita por derivação, o princípio do fruto da árvore envenenada, subsistirá se há nexo de causalidade entre o meio ilícito que foi

---

[92]DINAMARCO, Cândido Rangel. **Nova Era do Processo Civil**. 4. ed. São Paulo: Malheiros, 2013, p. 103.
[93]RANGEL, Paulo. **Direito Processual Penal**. 20. ed. São Paulo: Atlas, 2012, p. 365.

utilizado e a ligação entre a prova que está sendo apresentada, visto que, se a prova foi apresentada por meio independente da ilicitude cometida, essa será válida [94].

A verdade processual tem que ser clara, limpa, não dando nenhuma evasão para a dúvida no processo, para que o processo consiga chegar a um ideal justo.

Sem dúvidas as provas são a base do processo penal, pois, só através delas se elucidará os fatos. As provas traçam o caminho para que o julgador de forma motivada tome a sua decisão.

Em face dos crimes virtuais, as provas têm um caráter peculiar, visto que, esse tipo de delito não possui um campo real de atuação. Sendo o universo virtual um campo de infinitas possibilidades dificulta ainda mais a investigação, a coleta de material probatório e a identificação da autoria, têm maior complexidade para serem colhidas.

No capítulo a seguir analisaremos como é a atuação das provas no mundo virtual, os desafios enfrentados e as possíveis soluções para esse tipo de delito.

[94]RANGEL, Paulo. **Direito Processual Penal**. 20. ed. São Paulo: Atlas, 2012. p. 367.

4 DA PROVA NOS CRIMES VIRTUAIS

A evolução tecnológica possibilitou uma mudança na sociedade, nesse mesmo ritmo também são as mudanças delituosas. Marcelo Crespo cita que: “a evolução tecnológica da sociedade supõe uma evolução tecnológica dos ilícitos, tanto nos meios quanto nos objetos” [95].

Em meio a essa diversidade delitiva, as dificuldades de comprovação do fato criminoso é um desafio para o Estado, que precisa acompanhar todos os avanços tecnológicos e usá-los para combater o cibercriminoso.

Nesse capítulo analisaremos o sistema de provas virtuais, os desafios enfrentados em face da coleta probatória e identificação da autoria, como possíveis soluções encontradas na doutrina e na legislação.

4.1 A Ótica das Provas Virtuais

A prova no Processo Penal Brasileiro pode ser conceituada como: Um conjunto de ações praticadas pelas partes destinadas a comprovar em juízo a ocorrência ou inocorrência do fato, a veracidade ou não de uma informação. Demonstrando que: “é todo e qualquer meio de percepção empregado pelo homem com o objetivo de comprovar a veracidade de uma alegação” [96].

O elemento probatório é dividido em cinco elementos característicos e distintos entre si:

> 1-a obtenção da prova consiste na busca de elementos de prova que serão postos ao juízo por meio dos instrumentos de busca disciplinados em lei; 2-a proposição da prova, que se consubstancia na indicação pelas partes ao juiz dos meios de provas que se pretenderá no processo; 3- da admissibilidade da prova, por meio da qual o magistrado defere ou indefere os meios de provas anteriormente propostos; 4- a produção da prova em sentido estrito, meio que viabiliza a introdução da prova no processo penal; e 5-a valoração da prova, pelo qual o magistrado sopesa as provas produzidas no processo e valora, de acordo com cada caso concreto, aquelas que se mostram com mais ou menos “valor” diante das argumentações das partes e diante do que se convenceu para finalmente tomar sua decisão [97].

[95]CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Editora Saraiva, 2011, p. 159.
[96]CRESPO, Marcelo Xavier de Freitas, op. cit., p.144.
[97]AROCA, Juan Montero. **La prueba e nel proceso civil.** 4. ed. Madrid: Thomson Civitas, 2005, p. 284.

O mesmo paradigma coexistirá quando o assunto é prova digital, neste sentido, haverá equidade com todo o ordenamento jurídico, mesmo sendo provas peculiares, por sofrerem modificações a todo instante.

A prova digital é descrita por Silva Rodrigues como:

> Qualquer tipo de informação, com valor probatório, armazenada em repositório eletrônico-digitais de armazenamento, ou transmitida em sistemas e rede informática ou redes de comunicações eletrônicas, privadas ou publicamente acessíveis, sob a forma binária ou digital[98].

Por sua vez, Vera Dias apresenta uma noção que consideramos mais elucidativa classificando-a como a "informação passível de ser extraída de um dispositivo eletrônico (local, virtual ou remoto) ou de uma rede de comunicações. A prova digital, para além de ser admissível, deve ser também autêntica, precisa e concreta"[99].

O crime Virtual tem característica diversa dos crimes comuns, pois, o grau de dificuldade para sua investigação e comprovação dos fatos é maior do que nos crimes comuns, sendo necessárias perícias especializadas e técnicas para ser possível rastrear e identificar sua autoria.

Entendemos que, em um meio tão variado de invasões cibernéticas e de ataques constantes assim que acessamos o meio virtual, o que gera a maior dificuldade é encontrar de onde partiu a invasão e quem nos atacou. A existência de uma responsabilidade criminal para garantir a segurança jurídica, só poderá ser concretizada se houver certeza da autoria e da prática do ilícito.

A sensação de impunidade em face aos cibercrimes é visível nas vítimas, pela dificuldade Estatal encontrar a autoria do delito. A despeito disso ilustríssimo Doutor em Tecnologia Ricardo José de Souza Silva comenta:

> Como temos várias camadas de internet, as informações podem ser tornar armas para os infratores que cometem delitos virtuais, pois fica a sensação de impunidade, por um lado por nossa limitação de ação frente ao

---

[98]RODRIGUES, Benjamim Silva.**Direito Penal Parte Especial**.Tomo I, Direito Penal Informático-Digital, Contributo para a Fundamentação da sua Autonomia Dogmática e Científica à Luz do novo Paradigma de Investigação Criminal: a Ciência Forense Digital e a Prova Digital. Coimbra Editora, Limitada. ISBN: 978-989-95779-5-4.

[99]DIAS, Vera Marques.A Problemática da Investigação do Cibercrime. Data Venia, **Revista Jurídica Digital**, Ano 1, n. º 1, Julho-Dezembro 2012, ISSN 2182-8242.

> especialista infrator no meio virtual, por outro lado a expansão do estado de “nada acontece por aqui”, portanto, os atos delituosos se expandem exponencialmente[100].

Os obstáculos encontrados na investigação, e a escassez de provas que demonstrem que aquele ilícito subsistiu, e quem seria o agente ativo causador do dano, é um desafio a ser vencido, pois, na maioria das vezes essa prática não deixa rastros os quais possam ser levados a juízo.

O Estado tem seu papel regulador auxiliando a vida em sociedade, pois, o que acontece no mundo virtual tem impacto direto no mundo real, nas palavras de Ricardo Silva:

> O processo de regulação na rede virtual procura organizar o fluxo das ações das pessoas, suas atitudes e consequências. Não obstante, tais informações armazenadas, por autorização pessoal do contratante do serviço, podem afetar sua vida no mundo real, inclusive proporcionando a propagação de informações sigilosas, para instituições financeiras e agentes de consumo, o que ocasiona, por vezes, situações desconfortáveis, sobretudo no âmbito social[101].

Devido à obscuridade que a rede virtual possui, o autor do delito conquista o anonimato, outro ponto analisado, é a fragilidade das provas virtuais, pela facilidade de perda e danos na ocasião da coleta pericial, o momento da investigação é crucial para descobrir o criminoso, portanto, o conhecimento tecnológico dos operadores do Direto deve ser igualado ou mais atualizado do que o do criminosos, a fim de descobrir o autor do cibercrime.

No mesmo sentido Marcos Ferreira Lima discorre:

> Nesse tipo de investigação o objetivo é descobrir o endereço IP (*Internet Protocol*) do computador dentro de uma rede. E nem sempre isto será suficiente, pois há casos em que um único computador sirva a mais de uma pessoa, sendo então necessário identificar quem realmente o utilizou para a prática delituosa. Na apuração dos chamados crimes digitais, informáticos ou cibernéticos, ou de infrações penais praticadas mediante o uso de microcomputadores, os peritos costumam empregar a técnica “post-mortem”. Ou seja, o sistema é examinado após o desligamento da máquina, situação em que cabe ao perito proceder à duplicação das mídias e à avaliação de evidências armazenadas e/ou recentemente apagadas [102].

---

[100]SILVA, Ricardo José de Souza. **Delito Virtual**: Um diálogo sobre as transgressões online do mundo real. Delictæ: Revista de Estudos Interdisciplinares sobre o Delito. Volume 2. Número 4. Jan.-Jun./2018 Belo Horizonte: Centro de Investigações Interdisciplinares sobre o Delito, 2018. Semestral ISSN: 2526-5180 (eletrônico). Direito – II. Periódicos – III. Brasil.

[101]Ibidem. p. 263.

[102]LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computacional**. São Paulo: Editora Atlas, 2011, p. 6.

A velocidade surpreendente em que os conteúdos aparecem e somem na rede virtual, faz com que a consecução da investigação penal, exerça o papel garantidor para a elucidação do crime, mas, a investigação, esbarra nas garantias constitucionais aos Direitos de privacidade e do sigilo dos meios de comunicação, portanto, as provas ao serem colhidas obedecerão alguns critérios.

Na *International Hi-Tech Crimeand Forensic Conference*, realizada em Outubro de 1999, em Londres, o *Scientific Working Groupon Digital Evidence* apresentou definições, *standards* e princípios relevantes, a fim de demonstrar a comunidade forense internacional a natureza da prova digital e o caminho investigativo a percorrer, de forma que possa garantir a sua força probatória, sem esbarrar nas garantias fundamentais[103].

Uma dessas diretrizes diz que a prova virtual deverá a fim de garantir a sua integridade, apresentar uma linguagem simples, de forma que seja aplicada pela generalidade, mantendo apenas os termos técnicos considerados fundamentais e específicos.

Para garantir a conservação da prova, os técnicos forenses têm seguido o padrão determinado pelo SWGD (*Scientific Working Group On Digital Evidence*), colocando as provas colhidas no repositório de material forense em âmbito mundial, onde existem registros de documentos sobre vários assuntos, como vídeos, áudios e imagens digitais, sendo esses documentos, não fixados a uma única máquina operacional, justamente para garantir a proteção à possíveis ataques dos cibercriminosos[104].

Isso evidencia que o crime virtual tem um viés próprio e adequação no modelo internacional é necessária em face da investigação, de modo que, seja admitida em outros países relacionados com o crime em questão, pela natureza transfronteiriça do crime[105].

O espaço virtual é vasto, visando à melhor maneira de alocar cada procedimento usado, institui assim categorias que fazem uma distinção entre o elemento material de um sistema de computador e hardware (evidência eletrônica)

---

[103]FBI.gov isan official site ofthe U.S. government, **U.S. Department of Justice**.Disponível em: https://www.fbi.gov/about-us/lab/forensic-sciencecommunications/fsc/april2000/swgde.htm/. Acesso em: 05 abr. 2019.

[104]**CAIXETA**, T. F. G, Revista Segurança Digital – 9° Edição, 2012. Disponível em :https://periciacomputacional.com/pericia-digital/. Acesso em: 22 mar. 2019.

[105]GANDINI. João Agnaldo Donizeti, SALOMÃO, Diana Paola da Silva e; JACOB Cristiane. **A Validade jurídica dos documentos digitais**. Busca Legis.ccj.ufsc.br1 July 2016. Acesso em: 25 mar. 2019.

ou as informações contidas na máquina operacional (evidência digital). Essa distinção é útil no momento de projetar os procedimentos corretos para tratar cada tipo de evidência, criando um paralelo entre a cena de crime físico e a digital[106].

Em detrimento da necessidade de atualizar as formas de apuração dos crimes praticados por meios informáticos, surgiram às perícias especializadas, que coletam as informações dos dispositivos informáticos para uma posterior apuração, essa submissão a perícias técnicas tem sido até então, o melhor método para a apuração dos fatos.

A prova virtual segue critérios rigorosos para garantir a sua integridade e ter força probatória, dando estabilidade a investigação. É fundamental, que seja uniforme a produção dessa prova em todas as fases do processo forense digital, para que a prova seja admitida no tribunal e ao mesmo tempo que impede falhas na força probatória que no futuro venha por em risco as garantias individuais e os direitos fundamentais do indivíduo, como também, seja suficiente para encontrar e punir o cibercriminoso[107].

Por ser a prova digital instável e passível de mutabilidade devido a sua natureza específica, torna assim mais difícil a sua apreensão. São inúmeras as situações em que o investigador obtém uma prova e mais tarde observa que a prova obteve modificações consideráveis de maneira parcial, conservando apenas alguns aspectos ou modificação de maneira total, perdendo todas as suas características neste sentido, perde a força probatória[108].

O cibercrime caracterizado pela periculosidade e diversidade, gerando uma maior dificuldade para a sua averiguação, como nas questões de identificação e comprovação do fato/crime.

4.2 A Identificação do Cibercriminoso.

A busca pela reconstrução da verdade é o principal objetivo da prova judiciária, a ligação existente entre o fato verdadeiro, e a comprovação da ocorrência

---

[106]DEL PINO ' Dr. Santiago Acurio. **Manual de Manejo de Evidencias Digitalesy Entornos Informáticos**. Uruguai. s.a. p. 03

[107]OLIVEIRA, Eugênio Pacelli. **Curso de Processo Penal. Rio de Janeiro**. Úmen. Juris, 2012, p.328.

[108]GANDINI, João Agnaldo Donizeti, SALOMÃO, Diana Paola da Silva e; JACOB Cristiane. A Validade jurídica dos documentos digitais. BuscaLegis.ccj.ufsc.br1 July 2016. Acesso em: 25 mar. 2019.

no devido espaço e tempo, é o maior desafio da investigação, portanto, o material colhido durante a investigação terá de manter-se intacto, atingindo assim o seu efeito probatório diante do julgador[109].

Quando se trata de crime virtual, a correta identificação do autor é a matéria que causa maior preocupação para a investigação, a imputação objetiva da autoria é extremamente difícil, uma vez que, a ausência física do sujeito dificulta a identificação.

Existe uma necessidade Estatal em traçar um perfil dos praticantes do cibercrime, por haver uma maior facilidade em burlar a lei no ciberespaço, os criminosos com maestria usam a tecnologia e o conhecimento informático a seu favor, burlando sua localização[110].

A individualização do infrator penal é uma presunção específica para que o processo judicial seja instaurado, a ideia preconcebida de que senão houver uma presença física é impossível de chegar a autoria, é deveras errônea, pois, existem métodos e meios os quais se usados corretamente identifica o cibercriminoso.

O anonimato é uma das características no cibercrime, pois, o ambiente virtual proporciona ao indivíduo criar, transformar e refazer a sua identidade, com isso há uma maior atração dos criminosos pelo acesso livre e direto a rede mundial de computadores[111].

A princípio, o anonimato existe, mas, não é totalitário, é apenas aparente, pois, existem métodos de chegar ao autor do delito. Cada aparelho eletrônico com acesso a internet tem uma identidade própria conhecida como IP (*Internet Protocol*) ou protocolo de internet, essa identificação são sequências compostas de números, formando assim um endereço, que é atribuído individualmente tal quanto uma digital humana, não existindo nenhuma outra igual[112]. Assim como nós possuímos o R.G., os computadores possuem o I.P., capazes de identificar a máquina que está acessando a rede.

São números fornecidos pelo provedor de acesso que possibilita determinar o local da máquina e dessa forma comprovar se foi dela que partiram os comandos da

---

[109]TAVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Curso de Direito Processual Penal**. Salvador: Jus Podivm, 2014, p. 402.
[110]MALAQUIAS, Roberto Antônio Darós.**Crime Cibernético e Prova** – A investigação criminal em busca da verdade. Curitiba: Juruá Editora, 2012, p. 66.
[111]COLLI, Maciel. **Cibercrimes.** Limites e perspectivas à investigação policial de crimes cibernéticos. Curitiba: Juruá Editora, 2010, p. 347.
[112]PINHEIRO Patrícia Peck. **Direito Digital**. São Paulo: Editora Saraiva, 2013, p. 305.

ação criminosa. Na maioria das vezes, em a máquina se conecta a rede receberá um endereço de IP diferente, mas algumas conexões como um *Speedy* (veloz), não muda depois de fornecido um número de IP, mesmo que o computador desconecte-se e volta a navegar posteriormente[113].

Essa identidade permite coligar a máquina que foi utilizada na prática do delito, como também, a vítima, pois, esse endereço do IP descreve o tráfego do acesso feito pelo usuário em um determinado período.

Diferente da identificação do mundo "real", onde primeiramente observa às características físicas do autor, no mundo virtual a identificação é numérica, buscado primeiro identificar a máquina usada para cometer o delito e consequentemente tentar identificar o sujeito[114].

Outras maneiras existem para alcançar o cibercriminoso usando os registros de navegação, os registros servem para identificar os locais acessados pelo usuário e os serviços que foram utilizados. Sendo possível identificar a autoria, caso o acesso seja realizado pelo servidor *proxy* e feito de forma direta, isto é, sem a utilização de programas específicos que matem o anonimato. Ainda existe a dificuldade de alguns cibercriminosos burlarem o sistema tradicional da rede, utilizando o IP de um servidor hospedeiro, deixando quase impossível saber de que endereço partiu o crime.

O desafio a ser vencido nos crimes virtuais é a possibilidade de identificar o agente ativo do delito e identificar a origem da comunicação, isto é, vincular IP de onde partiu esses dados à quem estava utilizando o computador naquele espaço/tempo, visto que, a pessoa que utiliza pode não ser o proprietário do equipamento.

Neste sentido, o cibercriminoso a fim de inibir a identificação além de fazer uso de programas especiais em manutenção do anonimato, usufrui dos espaços públicos, utilizando de *Cybercafés*, bibliotecas públicas e demais espaços cujo acesso é livre[115].

Na investigação a quebra dos sigilos do IP é solicitado as concessionárias provedoras de Internet, com o objetivo identificar o dia e a hora do cometimento do

---

[113]COELHO, Ana Carolina Assis. **VIRTUAIS:** análise da prova. Disponível em: http://intertemas.toledoprudente.edu.br/ind.ex.php/Juridica/article/view/827/804, Acesso em: 22 abr. 2019.
[114]COLLI, Maciel. **Cibercrimes**. Limites e perspectivas à investigação policial de crimes cibernéticos. Curitiba: Juruá Editora, 2010. p. 45.
[115]PINHEIRO, Patrícia Peck. **Direito Digital**. São Paulo: Editora Saraiva, 2013.308

crime, traçando assim, um perímetro para tentar identificar a máquina e o autor, servindo de base para a investigação criminal[116].

Para a instauração do inquérito policial é necessário que o indício de autoria seja sólido, na hipótese de invasão seja para bisbilhotar, destruir ou furtar senhas ou cometer qualquer outro crime, somente será possível a abertura de um inquérito se a identidade do autor for confirmada, dando causa a uma ação penal concreta.

Neste sentido a tecnologia da informação traz maneiras de auxiliar a descoberta identidade do usuário, como teclado infranumérico, cartão de identificação, cartão de proximidade ativa e passiva, biometria, geometria da mão, impressão digital, leitura de retina ou íris, identificação de face, reconhecimento de voz e reconhecimento de caligrafia. Todos esses podem ser usados em locais públicos ou privados para identificar o usuário.

A correta individualização e uma certeza de autoria poderão dar a ação penal provas suficientes para que o poder Estatal incida sobre o indivíduo.

Roberto Maquias diz que:

> O Estado não pode estigmatizar o indivíduo e tampouco alcançar pessoas abstratas com meras inferências. A perfeita identificação do autor e a correta delimitação da infração cometida são essenciais para se punir o criminoso virtual principalmente, quando se considera o ambiente virtual em que o crime foi praticado, caracterizado pela ausência da presença física do infrator[117]

Demonstrar autoria com o exame de corpo delito poderia evitar erros técnicos no julgamento e garantir uma lógica processual, a realização do exame é uma regra processual quando os crimes não deixam vestígios, o Artigo 158 do Código de Processo Penal diz que: “Quando a infração deixar vestígios será indispensável o exame de corpo delito, direto ou indireto, não podendo supri-lo a confissão do acusado” [118], servindo como um laudo pericial do crime.

No Direito atual, a identidade digital é um assunto de grande relevância, porém, a falta de uma lei específica e um entendimento sólido e uniforme dá ensejo as mais variadas interpretações no poder judiciário. Quando o magistrado se depara com o assunto cibercrime, uns entendem que a identificação da autoria só será

---

[116]PINHEIRO, Patrícia Peck.op. cit., p. 309.
[117]MALAQUIAS, Roberto Antônio Darós.**Crime Cibernético e Prova** – A investigação criminal em busca da verdade. Curitiba: Juruá Editora, 2012, p.78.
[118]BRASIL. Decreto-Lei Nº 3.689, 3 de outrubro de 1941. **Código de Processo Penal**, 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm. Acesso em: 30 mar. 2019.

válida se houver certificado digital da IPC-Brasil, outra interpretação é só com a só com assinatura de digital, e alguns juízes a senha digital é suficiente para a comprovação dessa identidade[119].

Inserir mecanismos automáticos de localização e inibição imediata das práticas ilícitas virtualmente, também seria um grande avanço para identificação do cibercriminoso e sua persecução criminal.

Patrícia Peck Pinheiro afirma que a questão da prova de autoria é um dos grandes desafios do Direto na era digital, e dá uma nova forma para a possível identificação do autor:

> "A identificação do criminoso cibernético, de maneira mais inequívoca, só é possível através do uso da biometria que corresponde à utilização de características fisiológicas mensuráveis para autenticar um usuário tais como a impressão digital ou o reconhecimento facial[120].

Isto significa dizer, que a análise do infrator penal é uma das únicas formas seguras para identificar autoria, rastros como, elementos corporais deixados na cena do crime, quando o sujeito pára e acessa o mundo virtual, é um meio seguro de identificar quem cometeu o delito.

Não obstante, na investigação de um crime virtual correlacionar o endereço do IP com a máquina usada na prática do crime e essa máquina com o autor, é a dificuldade maior da investigação, consequentemente, ter certeza que essa titularidade é daquele sujeito que operou aquela determinada máquina, naquele espaço-tempo que o delito foi cometido é problemática enfrentada pela investigação.

A atribuição de um resultado juridicamente relevante nos crimes virtuais aponta para teoria da imputação objetiva, que atua por meio de uma conduta de risco que pode causar lesão ou ameaça a um bem tutelado. Acerca dessa teoria Leandro Vilela Brambilla comenta que:

> No âmbito do fato típico, deve-se atribuir ao agente apenas responsabilidade penal, não levando em consideração o dolo do agente, pois este é requisito subjetivo e deve ser analisado somente no que tange a imputação subjetiva[121].

---

[119]FIORILLO, Celso Antonio Pacheco. **Crimes no meio ambiente digital**. São Paulo: Saraiva, 2013, p. 227.
[120]PINHEIRO, Patrícia Peck. **Direito Digital**. São Paulo: Editora Saraiva, 2013, p. 118.
[121]BRAMBILLA, Leandro Vilela. **No que Consiste a Teoria da Imputação Objetiva.** Disponível em https://lfg.jusbrasil.com.br/noticias/1781169/no-que-consiste-a-teoria-da-imputacao-objetiva-leandro-vilela-brambilla. Acesso em: 05 mai.de 2018.

Incube ao legislador procurar meios eficazes e que sejam viáveis na busca do autor do crime virtual, verificar a periculosidade desses autores em razão do alcance incalculável de vítimas, e as particularidades nesse tipo de infrator.

4.3 Pericias nos Crimes Virtuais

Como o principal objetivo da prova é a reconstrução da verdade, uma ligação consistente entre o autor e a realidade histórica, confirmaria que o fato investigado no processo aconteceu e que o sujeito que está sendo investigado é o autor do delito.

As provas servem de auxílio para o magistrado fundamentar sua decisão, analisando a materialidade das provas e dos indícios da autoria formando um conjunto probatório sólido, e assim chegar a uma sentença condenatória ou absolutória.

Pela característica dessa modalidade criminosa, surge à necessidade de especialistas com amplo conhecimento de segurança de informação, computação, direito digital e áreas afins, profissionais dotados de conhecimento científico e tecnológico, sendo assim, a única forma de elucidar os crimes na rede.

Os métodos utilizados na ciência forense nos crimes físicos são os mesmos métodos adotados nos crimes virtuais. Tais métodos consistem na aquisição, preservação, análise e apresentação de evidência.

Esse dinamismo acarreta nos peritos uma maior responsabilidade, além de capacitação especial, pois sendo um crime não convencional, um simples vestígio perfaz um caminho no qual o cibercriminoso trilhou. Uma evidência digital como um histórico da internet, uma conversa no *chat*, e até mesmo arquivos excluídos intencionalmente, já seria um meio de prova [122].

Diante do inquérito policial a materialidade dos vestígios para a construção da prova deverá ser sólida e eficaz. O objetivo da investigação é o de reunir maior número de elementos que tenham qualidade relevante para o efeito comprobatório, determinando assim que o fato ocorrido é típico, culpável e punível.

---

[122]DODGE, Raquel Elias Ferreira, **Crime por computador** - Ministério Público Federal - Brasil coord. e org. II. Título. Roteiro de atuação: crimes cibernéticos. 2 ed. rev. - Brasília: MPF/2ªCCR, 2013, p. 139.

O RFC 3227 indica uma série de recomendações para que procedimento de coleta e preservação das provas no meio virtual, para que a prova seja:

> **1- Admissível**: está em plena conformidade com o ordenamento para ser apresentada em juízo.
> **2- Autêntica:** as provas devem sempre está relacionada ao fato/crime, portanto, a documentação tem que ter qualidade ao chegar ao julgador.
> **3- Completa:** o tipo de prova tem que estar conectada a fim de fornecer ao julgador os elementos que reconstrua o evento investigado.
> **4- Confiável**: não pode haver dúvida a autenticidade da evidência, como foi coletada manuseada e trazida ao processo.
> **5- Convincente:** a evidência deve ser apresentada de forma clara e organizada respeitando todas as características acima[123](tradução nossa).

Por ser o inquérito um procedimento administrativo cautelar, previsto no Artigo 6, III, do Código de Processo Penal tem o caráter provisório e inquisitorial, visto que, as autoridades policiais deverão colher as provas para esclarecimento dos fatos, com a finalidade de uma possível ação penal, por exemplo a ouvida de testemunhas de caráter provisório e as de caráter permanente como exames de corpo delito, apreensões e buscas nos locais suspeitos. O inquérito é um conjunto de medidas que a autoridade policial realiza afim de, coletar informações sobre a materialidade do fato[124].

Fica claro que a coleta de informações no inquérito policial não pode ser confundida como prova, pois, o princípio basilar do processo é o contraditório, isto é, se uma parte produz uma prova à outra além de ter direito de defesa sobre aquela prova apresentada também poderá produzir prova em contrário, sendo assim, o contraditório é uma condição para a validade das provas[125].

O Código de Processo Penal passou a prever essa distinção entre elementos informativos e provas contidas na lei 11.690/2008·[126], em síntese essa lei diz que os elementos informativos não comportam ampla defesa e o contraditório, sendo isso um instituto para as provas. Os elementos informativos são colhidos durante a investigação, e as provas são utilizadas para levar os elementos de convicção,

---

[123]Internet FAQ Archives. **Guidelines for Evidence Collectionand Archiving:**RFC 3227. Disponível em: http://www.faqs.org/rfcs/rfc3227.html, Acesso em 30 mar. 2019.
[124]LOPES JR, Aury. **Direito Processual Penal e Sua Conformidade Constitucional. 8ª edição.** Lumen Juris. Rio de Janeiro, 2011, p. 116.
[125]LOPES Jr. Aury,DA ROSA Alexandre Morais; BULHÕES Gabriel, **Investigação defensiva:** poder da advocacia e direito da cidadania. Disponível em: https://www.conjur.com.br/2019-fev-01/limite-penal-investigacao-defensiva-poder-dever-advocacia-direito-cidadania, Acesso em: 01 mar.2019.
[126]BRASIL, **LEI 11.690** de 9 de Junho de 2008. Disponível em:http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Lei/L11690.htm. Acesso em 22 abr. 2019.

produzidas no curso do processo judicial, tendo assim, o contraditório e a ampla defesa[127].

Os elementos colhidos no inquérito são de natureza pré-processual servindo para informar, por esse motivo, adota um caráter de medida cautelar pessoal, real e provisório. A fase preliminar serve para firmar uma convicção, dando base a acusação de caráter público ou particular, auxiliando o magistrado no processo e na decretação de medidas cautelares, caso desejar, mas, não pode ser usado para a fundamentação da sentença, só em casos excepcionais Artigo 155, do Código de Processo Penal:

> O juiz formará sua convicção pela livre apreciação da prova produzida em contraditório judicial, não podendo fundamentar sua decisão exclusivamente nos elementos informativos colhidos na investigação, ressalvadas as provas cautelares, não repetíveis e antecipadas[128].

Para Aury Lopes Jr. o inquérito policial possui eficácia probatória limitada, uma vez que somente gera atos de investigação[129], sendo apenas levados em consideração os elementos trazidos na fase anterior ao processo quando esse se repetirem na fase processual, levando em consideração a ampla defesa e o contraditório, para assim serem convertidas como prova.

O legislador visado à existência de provas de caráter perecível, e que devem ser colhidas e catalogadas rapidamente sob o risco de desaparecerem, fez uma ressalva no Artigo 155 no Código de Processo Penal[130], essa ressalva influencia diretamente nos crimes virtuais por ter essa natureza perecível, levando em consideração a distinção entre provas não repetíveis e provas cautelares.

As provas não repetíveis são aquelas que não podem ser produzidas novamente, por ser passível de destruição, perecimento ou desaparecimento, já as provas cautelares, são aquelas sujeitas a risco de perecimento em razão ao decurso do tempo. As provas antecipadas devem ser usadas em casos excepcionais, pelo atributo de urgência conferido a ela.

---

[127] LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computaciona**l. São Paulo: Editora Atlas, 2011, p.123

[128]BRASIL, Decreto-Lei Nº 3.689, de 3 de Outubro de 1941.**Código de Processo Penal**, 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm Acesso em: 30 mar. 2019.

[129]LOPES JR, Aury. **Direito Processual Penal e Sua Conformidade Constitucional.** 8. ed. Lumen Juris. Rio de Janeiro, 2011, p. 143.

[130]BRASIL, Decreto-Lei Nº 3.689, de 3 de Outubro de 1941.**Código de Processo Penal**, 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm Acesso em: 30 mar. 2018.

O Ciberespaço e a *Web* são formados por diferentes sistemas, que podem ser ou não, conectados ao grande *backbone* (espinha dorsal) formando o sistema de tráfego da internet.

A movimentação do tráfego da internet consiste em enviar, receber, armazenar, transferir dados e informações, contudo, não há regras de uso, em contraponto o legislador obriga as operadoras de internet guardar os registros de acesso, podendo ser guardados na máquina física ou no provedor de acesso[131].

Um dos principais expoentes da ciência forense é a coleta de dados para a formação de evidências, as quais servirão para fins de prova em uma investigação criminal. Da mesma maneira acontece nos crimes virtuais, tanto na investigação quanto no processo, a coleta de dados é necessária e a única maneira de determinar como aconteceu o fato.

As garantias e os direitos fundamentais desempenham na investigação um contexto de função negativa, visto que, dão limite ao investigador no âmbito virtual, isso fica ainda mais claro, pois, na investigação forense dentro do espaço virtual é mais complexa, e acaba infringindo garantias individuais, como por exemplo, a privacidade.

A análise feita nos cibercrimes é minuciosa, pois, são necessários peritos especializados, considerando que os criminosos utilizam de programas que de alto nível, que na maioria das vezes só é conhecido por especialistas em programação. Esses programas trazem consigo um único objetivo, mascarar o indivíduo e fazer com que esse, permaneça em anonimato[132].

Não é sempre os vestígios das provas estão nos locais onde o crime foi consumado, visto que, a transitoriedade de registros magnéticos é constante, neste sentido a realização de coleta das provas deve ocorrer dentro de um curto período de tempo, a fim de evitar que detalhes sobre a prática do crime sejam perdidos[133].

Diante disso, uma coleta de provas em âmbito virtual deve ser rápida, pois, os meios que encobrem o delito são eficazes. Os programas que modificam a máquina

---

[131]FIGUEIREDO, Jonathan. **História da Internet**. 2013. Disponível em: jonathanfoste.blogspot.com/2013/08/historia-da-internet-acesso-internet.html. Acesso em: 29 abr. 2019.

[132]GRECO FILHO, Vicente**. Algumas observações sobre o direito penal e a internet**. Boletim do IBCCrim. São Paulo. Ed. Esp., ano 8, n. 95, out. 2000.

[133]COLLI, Maciel. Cibercrimes. **Limites e perspectivas à investigação policial de crimes cibernéticos**. Curitiba: Juruá Editora, 2010, p.135

encobrindo os rastros são esmeros, se caso a investigação for realizada posteriormente não haveria como identificar o delito, nem o sujeito.

Com programas do tipo o *disk-wiping* instalado nas máquinas, facilitaria a comprovação do fato, pois, esses programas permite a gravação de informações no mesmo espaço em que antes existia um dado deletado, mas, esse dado deletado permaneceria armazenado no disco rígido da máquina, sem referência de localização[134].

Maciel Colli afirma que o problema para investigação criminal surgirá quando os vestígios (arquivos, dados) deixados pela prática do crime forem deletados e o espaço por ele ocupado for novamente ocupado por outros dados, impossibilitando seu rastreamento pela perícia especializada mesmo se utilizando das ferramentas forense[135].

A forma em que os dados informáticos são processados impedem na maioria das vezes detectar as atividades realizadas, dando evasão para fraudes nas informações pelo uso de manipulação nos programas. Sustentando esse exponencial perigo em face dos crimes virtuais, alguns procedimentos são necessários, para um resultado mais eficaz, pois, esse tipo de prova são efêmeras e voláteis, e podem não surtir efeitos no futuro processo caso não sejam coletadas de maneira diferenciada.

A produção antecipada de provas é apontada como um fator determinante e necessário quando se trata do cibercrime. Por se tratar de uma medida excepcional, há pressupostos impositivos de extrema relevância para que essa medida seja tomada e aceitas em juízo.

Poderá ser realizada nos casos em que a prova não possa ser repetida em juízo, todavia estará condicionada a eficácia e aos requisitos mínimos da fiel reprodução durante o processo, da possibilidade de defesa, do contraditório e da jurisdicionalidade[136].

Analisamos que diante dos crimes cibernéticos, existe uma necessidade fazer uso de provas obtidas no inquérito pela particularidade da natureza do crime, provas

---

[134]NOVAIS, Rafael. **HD**: Entenda onde seus dados são armazenados. mai.2015. Disponível em:https://www.psafe.com/blog/hd-entenda-onde-seus-dados-sao-armazenados/. Acesso em: 30 fev. 2019.

[135]COLLI, Maciel. Cibercrimes. **Limites e perspectivas à investigação policial de crimes cibernéticos**. Curitiba: Juruá Editora, 2010, p.130-140.

[136]TALAMINI, Eduardo. mar. 2016.**Produção antecipada de prova**.Disponível em: https://www.migalhas.com.br/dePeso/16,MI235462,51045-Producao+antecipada+de+prova. Acesso em: 22 Mar. 2019.

como: 1- Cautelares provas em que há um risco de desaparecimento do objeto da prova em razão do decurso do tempo; 2- Provas não repetíveis, aquela que não tem como ser novamente coletada ou produzida, em virtude do desaparecimento, destruição ou perecimento da fonte probatória; 3-Provas antecipadas, aquelas produzidas com a observância contraditórias para a prova, perante o juiz natural, em momento processual distinto, antes do início do processo, em virtude de situação de urgência e relevância[137], esclarecendo que todas dependem de autorização judicial.

As provas apresentadas aos magistrados serão extraídas de registros eletrônicos com histórico de conexões de acesso, utilizando as técnicas forenses digital em parceria com a polícia e os demais operadores da justiça[138].

A integração entre técnicos especialistas e o Estado, fez progredir a capacidade defensiva e ofensiva de enfrentamento ao cibercrimes. Com o auxílio das inovações tecnológicas de controle, em relação à identificação, investigação e monitoramento minimizou o impacto dos ataques cibernéticos.

As tecnologias de proteção são descritas como um selo de autenticação, no qual, se faz o uso de senha, *cookies* e marcadores digitais, para garantir certo reconhecimento do usuário. No entanto, as tecnologias de monitoramento são baseadas na recognição, localizando o indivíduo, controlando as atividades do usuário e permitindo assim um manejo e uma identidade acerca da pessoa, dando pretexto a uma vigilância constante[139].

O problema da identificação prévia do criminoso é o quanto isso interfere na privacidade e nos direitos e garantias individuais, existem limites impostos ao Estado na questão de invadir a privacidade do indivíduo, portanto, há choque com as garantias de proteção e dignidade humana, nesse contraponto, a obtenção de uma prova como essa poderá ser considerada ilícita, visto que, estaria indo na contramão dessas garantias individuais, se contrapondo com o direito material já adquirido.

As elaborações de um banco de dados, através de resultado de uma identificação, monitoramento e acumulação de informações, poderão conjecturar um

---

[137]MACHADO, PATRÍCIA GOMES. **O Artigo 155 do CPP e os crimes de competência do júri.**Set. 2015. Disponível em: http://www.conteudojuridico.com.br/artigo,o-artigo-155-do-cpp-e-os-crimes-de-competencia-do-juri,54459.html. Acesso em: 22 abr. 2019.

[138]CAVALHEIRO, Renan. Jan. 2018. **Crimes Virtuais:** Investigação Forense de Golpes na Internet – Phishing. Disponível em:https://www.academiadeforensedigital.com.br/crimes-virtuais-phishing-forense/. Acesso em: 22 de abr. 2019.

[139]MARCONDES, José Sérgio.**Tecnologia de Identificação Aplicada no Controle de Acesso**. 2016. Disponível em: https://gestaodesegurancaprivada.com.br/tecnologias-de-identificacao/. Acesso em: 25 abr.2019.

perfil do cibercriminoso e ajudar a manter em observação, aquele que cometeu um ilícito na rede.

Esse banco de dados abriria espaço para o acompanhamento de certos indivíduos, fazendo uso de monitoramento das páginas acessadas na *web*, os rumos dos pagamentos de cartões de crédito, os *e-mails* enviados e recebidos e os demais acessos a rede, podendo traçar um perfil incriminador, de um possível delinquente, como também, esse tipo de monitoramento poderá afastar o reincidente de crimes praticados no ambiente virtual, lembrando que, essas ações para serem realizadas precisariam seguir o artigo 5º, inciso XII da CF/88.

A cooperação entre entidades públicas e privadas são necessárias, porque a entidade pública aplica a lei e a privada tem capacidade de mobilizar os meios tecnológicos para o exercício da função pública no combate à criminalidade[140].

Uma junção entre o Estado e diversos profissionais na área de defesa tecnológica, seria um grande passo a ser dado. A criação de uma base Nacional de Segurança Cibernética, conectados com o banco mundial de dados, é um passo a ser dado pela legislação brasileira, pois esse tipo de delito é transmundial, com essa conexão seria mais fácil alcançar os cibercriminosos e obter provas do delito, visto que, o crime na internet se dissipa e rompe as fronteiras internacionais.

Bechara explica a importância na obtenção de provas transnacionais:

> Aquela cujo meio de prova se encontra num Estado distinto ao da autoridade judicial competente, ou ainda quando os meios de prova de um mesmo fato se encontram em Estados diversos. Em outras palavras, a prova transnacional é aquela cuja fonte de prova encontra-se dentro dos limites da soberania de outro Estado, e que, portanto, requer a cooperação e o auxílio deste para a obtenção do dado ou elemento probatório[141].

A lei vigente adota como regra, o Art. 5º, caput, do Código Penal, que incide como será a aplicação da lei em caso dos crimes transfronteiriços. Rege a norma o Princípio da Territorialidade, segundo o qual se aplica a lei penal brasileira aos crimes cometidos no território nacional, ressalvados os casos do art. 7º, II, do mesmo diploma legal.

Neste sentido Francisco Toledo explana o seguinte:

---

[140]VERDELHO, Pedro. **Cibercrime e segurança informática**, Polícia e Justiça, série 3, n. 6 jul/dez..2005, p. 166 .

[141]BECHARA, Fábio Ramazzini. **Cooperação jurídica internacional em matéria penal:** eficácia da prova produzida no exterior. São Paulo: Saraiva,2012, p. 37-38

> São submetidos à lei brasileira os crimes cometidos dentro da área terrestre, do espaço aéreo, e das águas fluviais e marítimas, sobre as quais o Estado brasileiro exerce sua soberania, pouco importando a nacionalidade do agente. Porém, nos dias atuais, o conceito de território para fins de aplicação da jurisdição deve englobar também o espaço virtual, com todos os serviços de Internet prestados no Brasil[142].

É necessário que tomemos medidas preventivas, pois, a lei ainda é obsoleta. Uma unidade de lei em esfera internacional, em face aos crimes praticados na internet seria um grande avanço para, localizar e punir o cibercriminos nesse universo sem fronteiras. Nas palavras de Perpétua Almeida:

> A cibersegurança é uma novidade na Defesa Nacional, os planos e metas a serem alcançados como: capacitação tecnológica para que não dependa de tecnologia estrangeira; desenvolvendo nossos setores educacionais, industriais e militares na área virtual, andam em passos pequenos, mas o posicionamento da sociedade é absorver particularmente essas tecnologias de segurança, não esperando o posicionamento do poder estatal[143].

Deve também ser observada a atualização que deve ser feita na investigação probatória, é importante ressaltar a necessidade de contratação de peritos especialistas no campo forense computacional, para averiguar uma invasão no seu espaço virtual, como também, monitorar e proteger o cidadão de uma possível invasão.

O Estado deve atuar para dar mais segurança ao usuário na rede, e investir na atualização de equipamentos e em especialistas em técnicas forenses digital, visto que, a prova digital é instável e passível de mutabilidade.A natureza específica da prova digital torna mais difícil a sua apreensão. Verificam-se situações em que o investigador consegue uma prova, e mais tarde observa que a prova obteve modificações ou parcial ou total, perdendo o efeito probatório[144].

A prova digital tem característica de imaterialidade, com isso, atribui diretamente uma responsabilidade ao investigador forense, contudo, a coleta demanda de técnicas específicas pela complexidade e codificação existente, sob pena de perda das características da prova em si, ou a perda da força dessa prova no processo.

---

[142]TOLEDO, Francisco de Assis. **Princípios Básicos de Direito Penal**. São Paulo: Ed. Saraiva, 1991, p. 45

[143] ALMEIDA, Perpétua.**Estratégias de defesa nacional**: desafios para o Brasil no novo milênio/Perpétua Almeida e Luciana Acioly. – Rio de Janeiro: Ipea, 2014, p.204.

[144]GANDINI, João Agnaldo Donizeti .SALOMÃO,Diana Paola da Silva e Jacob,Cristiane. Jul. 2016.**A Validade jurídica dos documentos digitais.** Disponível em: http://www.ambito-juridico.com.br/site/index.php?artigo_id=4411&n_link=revista_artigos_leitura. Acesso em:30 abr.2019.

O manejo dessas provas sem os cuidados específicos poderá acarretar uma eventual modificação pelo próprio investigador no momento da coleta, alterando ou eliminando a prova, pelo fato de desconhecimento da presença dessa prova naquele ambiente específico.

De modo que, ao acessar a sistemas ou redes informáticas o investigador deverá munir-se de todas as técnicas e conhecimentos científicos, para dar uso de palavras-chave ou servir-se de técnicas de desencriptação, considerando os seguintes requisitos antes de iniciar um exame:

> 1-A urgência e a prioridade que o requisitante precisa das informações;
> 2-Outros tipos de análise forense, que podem precisar de cuidados com o item periciado;
> 3-Quais itens são potenciais fontes de informações no inventário de evidências;
> 4-Uma estratégia de análise deve ser de consentimento de todos os envolvidos, é preciso evitar conduzir uma análise na mídia original sempre que possível, utilizar-se de práticas, processos e procedimentos aceitos na atuação forense[145].

O exame deve ser realizado sempre de forma sistemática, tanto a nível lógico, quanto a nível físico. É muito importante que o perito tenha expertise e conheça várias técnicas a fim de saber qual a técnica que usará diante de um determinado cenário[146].

Para este propósito, foram criadas categorias fazendo uma distinção entre o elemento material de um sistema de computador ou *hardware* (evidência eletrônica) e a informações contidas no mundo virtual (evidência digital). Essa distinção é útil, pois, dar base ao perito, qual o procedimento correto será usado, para tratar cada tipo de evidência e criar um paralelo entre uma cena de crime físico e uma digital.

Neste contexto, o *hardware* refere-se a todos os componentes físicos de um sistema de computador, enquanto a informação refere-se a todos os dados, programas e mensagens de dados transmitidos usando o sistema de computador[147].

O procedimento correto é a quando ao se realizar uma coleta de imagem/cópia forense, averiguar sempre a integridade do material antes de ser enviado para o poder judiciário. O perito deverá descrever e documentar qualquer

---

[145]CAVALHEIRO, Renan**. Perícia Forense:** A profissão de Perito Digital está crescendo!.Mar. 2018 Disponível em: https://www.academiadeforensedigital.com.br/pericia-forense-perito-digital/.Acesso em:18 mai. 2019.

[146] LOPES, Petter. **Perícia Digital**.| Forense Digital, Perícia Forense Computacional. Dez. 2013. Disponível em: https://periciacomputacional.com/pericia-digital/. Acesso em: 22 mar. 2019.

[147]DEL PINO, Dr. Santiago**. Manual de Manejo de Evidencias Digitales y Entornos Informáticos.** Versión 2.0. s.n.

dano que eventualmente seja identificado, principalmente se prejudicar o laudo pericial, caso seja necessário, junte fotos a documentação mostrando a situação do material na hora da coleta. Além de usar esse modo de prevenção, deverá o perito documentar qualquer outra coisa análoga a investigação.

O *software* e o *hardware* utilizados na perícia devem ter a capacidade de efetuar bloqueio de escrita sobre a evidência, dando proteção a possíveis alterações do material durante o processo de criação da imagem/cópia. A perícia deve ser realizada *bit* a *bit*, ou seja, setor a setor, averiguando todos os *bits* existentes na mídia e fazendo cópias, evitando assim a perda desse material.

No caso específico das cópias forenses onde o conteúdo de uma mídia é copiado, um cuidado adicional deverá ser tomado, isto é, a mídia de destino onde serão copiados os dados de prova, deverá ser previamente esterilizada através de ferramenta de *wipe* (limpeza).

A legislação brasileira deverá desenvolver um procedimento adequado para a guarda das evidências, visto que a Lei 11.690/2008, que deu nova redação ao Art. 159, § 6º do Código de Processo Penal, determinando que:

> Havendo requerimento das partes, o material probatório que serviu de base à perícia será disponibilizado no ambiente do órgão oficial, que manterá sempre sua guarda, e na presença de perito oficial, para exame pelos assistentes, salvo se for impossível a sua conservação[148].

Assim sendo, todo material forense apresentado deve ser munido de técnicas de coleta e preservação e de técnicos especializados na área forense digital, para dar autenticidade as provas e não causar dúvidas quando levadas em juízo.

A tendência mundial é a cautela, com o intuito de não ferir os Direitos Humanos. Procurando se munir de inovações e especialistas com o objetivo de prevenir e combater os cibercriminosos, mas essa onda mundial não impede que os diversos sistemas jurídicos, pois as tradições culturais e sociais são diferenciadas em cada nação, exercendo assim, uma autonomia para que cada ordenamento jurídico se posicionarem conforme as suas necessidades[149].

---

[148]BRASIL, Decreto-Lei Nº 3.689, de 3 de outubro de 1941.**Código de Processo Penal**, 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm Acesso em: 30 mai. 2019.

[149]FÓRUM DE GOVERNANÇA DA INTERNET [livro eletrônico]: relatórios dos dez primeiros anos do IGF / Núcleo de Informação e Coordenação do Ponto BR ; [tradução Linguagem Idiomas]. - São Paulo: **Comitê Gestor da Internet no Brasil**, 2017. -- (Cadernos CGI.br Referências) 6,95 Mb ; PDF Título original: IGFs' chairsummaries Vários colaboradores. Bibliografia. ISBN 978-85-5559-055-9. Disponível em:

Isto demonstra que nenhuma legislação estrangeira deverá ser simploriamente copiada pelo Brasil visto que cada ordenamento jurídico passa a ter sua relevância com as experiências vividas por ele. Deveremos observar e usar nossas prioridades em combate ao crime virtual.

Sendo assim, é papel do ente público dar aparato para que sistema de provas seja eficaz, o Estado deve ter uma legislação atualizada, profissionais capacitados e equipamentos modernos, a fim de prevenir e elucidar os mais variados crimes virtuais.

Por fim, no mesmo parâmetro das propostas apresentadas nesse capítulo, então a proposta de um projeto de lei apresentadas pelo então Ministro da Justiça e Segurança Pública, Sérgio Moro, destacamos algumas que contribuem diretamente para as soluções apontadas em nossa pesquisa, vejamos:

> XVIII) Medidas para aprimorar a investigação de crimes:Mudança na Lei de Execução Penal (Banco Nacional de Perfil Genético):
> "Art. 9º-A. Os condenados por crimes dolosos, mesmo sem trânsito em julgado, serão submetidos, obrigatoriamente, à identificação do perfil genético, mediante extração de DNA - ácido desoxirribonucleico, por técnica adequada e indolor, quando do ingresso no estabelecimento prisional.§ 3º Os condenados por crimes dolosos que não tiverem sido submetidos à identificação do perfil genético, quando do ingresso no estabelecimento prisional, poderão ser submetidos ao procedimento durante o cumprimento da pena.§ 4º Constitui falta grave a recusa do condenado em submeter-se ao procedimento de identificação do perfil genético." (NR)
> Mudança na Lei n. º 12.037/2009 (Banco Nacional de Perfil Genético):
> "Art. 7º-A. A exclusão dos perfis genéticos dos bancos de dados ocorrerá no caso de absolvição do acusado ou, mediante requerimento, decorridos vinte anos após o cumprimento da pena no caso do condenado." (NR)
> Mudança na Lei n. º 9.296/1996 (interceptação telefônica):
> "Art. 9º-A. A interceptação de comunicações em sistemas de informática e telemática poderá ocorrer por qualquer meio tecnológico disponível desde que assegurada a integridade da diligência e poderá incluir a apreensão do conteúdo de mensagens e arquivos eletrônicos já armazenado em caixas postais eletrônicas." (NR)[150].

A aprovação desse projeto trará novos parâmetros no sistema de provas brasileiro, trazendo modernidade as leis vigentes em combate ao crime.

---

https://cgi.br/media/docs/publicacoes/1/CadernoCGIbr_Forum_de_Governanca_da_Internet.pdf. Acesso em 10 mai. 2019.

[150]PROJETO DE LEI ANTICRIME. **Anteprojeto de Lei Nº , de 2019**. Disponível em https://www.justica.gov.br/news/collective-nitf-content-1549284631.06/projeto-de-lei-anticrime.pdf. Acesso em 16 mai. 2019.

Esse projeto contribui diretamente na resolução dos crimes virtuais, modernizando o sistema de prova e quebrando as barreiras impostas na lei atual, pois, ele facilitaria na prevenção do crime e no monitoramento do cibercriminoso.

CONCLUSÃO

O crescente avanço tecnológico e a popularização da internet fizeram com que o legislador tenha dificuldade em tipificar algumas condutas delitivas, e consequentemente solucionar a grande maioria dos casos de crimes virtuais.

O presente trabalho acadêmico teve como objetivo maior identificar os desafios apontados pela doutrina em face ao sistema de provas nos crimes virtuais. Apontamos a problemática jurídica desde o momento da identificação da autoria, na obtenção e manutenção do material probatório como também, analisamos a legislação brasileira e a maneira que ela se comporta diante desse tipo de crime.

Como toda a evolução tem seu paralelo o ônus e o bônus, as ferramentas tecnológicas fazem parte do cotidiano da sociedade, no encalço dessa facilidade do mundo moderno traz consigo também novas práticas de delitos. Nessa evolução o

criminoso pode lograr êxito sem maiores esforços, pois, na maioria dos crimes virtuais apenas um computador, ou simples celular é utilizado como ferramenta para se chegar ao objetivo.

O processo penal é utilizado para levar os fatos até o magistrado, e a prova é o que leva o julgador a reconhecer se aquele fato realmente ocorreu. Por meios das provas que as partes envolvidas no processo irão narrar os fatos, a fim de, convencer o juiz da sua veracidade.

Considerando que os crimes virtuais têm características peculiares como volatilidade e efemeridade, há uma maior dificuldade de armazenar e assegurar a integridade das provas na investigação, pois, existe a necessidade de peritos especializados para coletar todo o material que servirá de base no processo.

No que tange os cibercrimes, a coleta das provas é o elemento essencial para se chegar a autoria do criminoso, as diversas maneiras em que se pratica crimes no universo virtual e as ferramentas usadas, dificulta ainda mais a extração das provas, por isso, uma perícia especializada é de suma importância para a extração e preservação dessa prova.

Existem maneiras de tentar evitar que dados essenciais para efeitos de provas se pecam, uma delas é a produção antecipada de provas. Prevista no Código de Processo Penal como medida excepcional, implica diretamente nas características do cibercrime, pois, muitas dessas provas não poderão ser replicadas em juízo, visto que, se perdem no conjunto espaço/tempo, lembrando que essas medidas têm que respeitar as garantias do contraditório e da ampla defesa.

Observamos também que, uma das dificuldades nesse tipo de delito é a identificação da autoria, uma vez que, o próprio ambiente do crime é virtual é caracterizado pela ausência de espaço físico, e isso facilita o anonimato, mesmo que, a ferramenta utilizada seja identificada, será difícil associar quem à utilizou.

Uma solução viável seria a utilização da biometria ou qualquer outro meio que tenha como extrair características fisiológicas do usuário, como também, o monitoramento dos cibercriminosos, praticarem delitos e a legislação brasileira em face à esses crimes.

Percebemos que existem diversas formas da violação do bem jurídico no meio virtual, e que o acesso as tecnologias auxiliaram o cometimento de novos delitos. O risco que a sociedade vive é constante, assim que adentra nesse vasto mundo da internet a sujeição de invasões em face do usuário, se tornam cada vez

mais diversificadas, sendo usadas para ferir a privacidade e levar vantagens indevidas a quem faz uso dessa conectividade.

A constante mudança dificulta a prevenção e repressão, uma vez que no mundo informatizado não há como mensurar qual a proporção do delito, quantos foram os agentes passivos e até mesmo quantos são os agentes ativos em um mesmo crime.

Vimos também que a legislação brasileira deu um grande passo criando leis específicas para os delitos em âmbito virtual, mas ainda existem questões a serem discutidas a fim de combater a criminalidade informática, que não param de evoluir.
Analisamos no segundo capítulo a Teoria Geral da Prova, considerando a importância das provas no processo, exemplificando os meios de provas, o objeto de provas, a classificação e o sistema que o ordenamento brasileiro utiliza para valorar essas provas no processo.

A perpetuação, a periculosidade e dinamismo dos crimes virtuais afeta diretamente a ciência probatória, com tudo isso, mesmo que seja evasiva a atuação do crime virtual, os princípios e as garantias voltadas ao indivíduo não podem deixar de existir apenas para elucidar esse tipo de crime mesmo que em casos excepcionais, o Direito do contraditório e ampla defesa não devem ser banalizados.

Trazendo a base do primeiro e do segundo capítulo, o capítulo três focas em questões peculiares do crime virtual. Analisamos nesse capítulo as relações específicas do sistema de provas no âmbito virtual, as questões relativas de identificação da autoria e os meios periciais utilizados nesses delitos.

A investigação é a base do processo, e diante da dificuldade de obtenção de provas no mundo da internet, procuramos uma solução visto a problemática na identificação da autoria, da dificuldade pericial em colher provas e da adequação legislativa em face a natureza transfronteiriça do crime.

Também por solução, apontamos a produção antecipada de provas como meio necessário a esse tipo de delito, pela característica de perecimento desse tipo de prova no decurso espaço/tempo, a biometria e coleta de material fisiológico para identificar o cibercriminoso, também, enaltecemos a perícia especializada nesse tipo de investigação, visto que, é necessário o uso técnico para a realização da coleta de dados, pois assim, garantiria a apreciação e validação das provas em juízo.

Os alvos dos cibercriminosos são variados e a cada dia são criadas novas infrações penais, um banco de dados como base Nacional em Segurança

Cibernética poderia ser criado tendo como referência parâmetros internacionais. Um sistema integrado tendo como componentes a sociedade, empresas de segurança, os institutos bancários, os centros de pesquisas, dentre outros órgãos se conectando entre si.

O banco de dados nacional estaria ligado com um banco de dados mundiais, assegurando mais a eficácia na identificação da autoria, posto que os crimes virtuais ultrapassam as fronteiras. Apontamos também, um projeto de lei em tramitação no parlamento que se assemelha a nossa solução, esse projeto modifica alguns trechos na legislação, deixando-a mais atual e eficaz.

Conclui-se que, a velocidade tecnológica e os mais variados mecanismos de comunicação, fez com que a cada dia se crie e se modifique os meios para cometer delitos e alcançar o anonimato.

Diante da problemática probatória levantada em nosso estudo, tentamos encontrar uma alternativa que impute ao Estado enxergar maneiras de adequação dentro desse meio rápido e em constante evolução, garantindo a proteção do indivíduo na sua privacidade, não desconstituindo os direitos e garantias já adquiridas.

REFERÊNCIAS

ABELLÁN, MarinaGascón. **Los hechos e nel derecho:** bases argumentales de la prueba. Madrid: Marcial Pons, 1999.

ALMEIDA, Perpétua.**Estratégias de defesa nacional**: desafios para o Brasil no novo milênio/Perpétua Almeida e Luciana Acioly. – Rio de Janeiro: Ipea, 2014.

AQUINO, José Carlos G. Xavier de. **A prova testemunhal no processo penal brasileiro**. 4.ed. São Paulo: Juarez de Oliveira, 2002.

ARANHA, Adalberto José Q.T. Camargo. **Da Prova no Processo Penal**. 7. ed. São Paulo: Saraiva, 2006.

AROCA, Juan Montero. **La prueba e nel proceso civil.** 4. ed. Madrid: Thomson Civitas, 2005.

BARBUENA, Lucas André. **Crimes Cibernéticos.** Publicado em 24 Mar. 2018. Disponível em: https://lucasbarbuena.jusbrasil.com.br/artigos/559759168/crimes-ciberneticos. Acesso em: 20 mar. 2019.

BECHARA, Fábio Ramazzini. **Cooperação jurídica internacional em matéria penal:** eficácia da prova produzida no exterior. São Paulo: Saraiva. 2012.

BERETTA, Pedro. **Sem Meios Eficazes,** Lei Carolina Dieckmann até atrapalha. São Paulo: Dublê Editorial, 2014. Disponível em: https://www.conjur.com.br/2014-mai-10/pedro-beretta-meios-eficazes-lei-carolina-dieckmann-atrapalha. Acesso em: 10 mai. 2018.

BRAMBILLA, Leandro Vilela. **No que Consiste a Teoria da Imputação Objetiva.** Disponível em https://lfg.jusbrasil.com.br/noticias/1781169/no-que-consiste-a-teoria-da-imputacao-objetiva-leandro-vilela-brambilla. Acesso em: 05 mai.de 2018.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 29 mar. 2018.

_____, L**ei nº 13.105,** de 16 de Março de 2015.Disponível emhttp://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.ht Acesso em: 17 de abr. 2018.

_____, Decreto-Lei Nº 12.737, de 30 de Novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos**; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 -Código Penal;e dá outras providências, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm Acesso em: 22 mar. 2018.

_____, Decreto-Lei Nº 12.965, de 23 de Abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato20112014/2014/lei/l12965.htm Acesso em: 10 mar. 2018.

_____, Decreto-Lei Nº 2.848, de 7 de Dezembro de 1940. **Código Penal**, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm> Acesso em: 15 mar. 2018.

_____,Lei nº 12.965, de 23 de Abril de 2014.**Marco Civil da Internet.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 22 de abr. 2018.

_____,Decreto-Lei Nº 3.689, de 3 de outubro de 1941.**Código de Processo Penal**, 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm Acesso em: 30 mar. 2018.

_____,Lei nº 8.069, de 13 de Julho de 1990. **Estatuto da Criança e do Adolescente. Disponível em** http://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em 16 de abr. 2018.

_____. **Lei11.690,** de 9 de Junho de 2008. Disponível em:http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Lei/L11690.htm. Acesso em 22 abr. 2019.

_____. Decreto-Lei Nº 2.848, de 7 de Dezembro de 1940. **Código Penal**, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em: 15 fev. 2018.

_____. Lei Nº 12.737, de 30 de Novembro de 2012.**Lei Carolina Dieckmann.**Disponível em :http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 25 abr. 2018.

_____**. Lei Nº 12.965,** de 23 de Abril de 2014.Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 27 abr. 2018.

_____.**Lei Nº 11.343,** de 23 de Agosto de 2006. Disponível em :http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11343.htm . Acesso em: 28 abr.2018.

CAIXETA, T. F. G, Revista Segurança Digital – 9° Edição, 2012., Disponível em :https://periciacomputacional.com/pericia-digital/. Acesso em: 22 mar. 2019.

CAVALHEIRO, Renan. Jan. 2018. **Crimes Virtuais**: Investigação Forense de Golpes na Internet – Phishing. Disponível em:https://www.academiadeforensedigital.com.br/crimes-virtuais-phishing-forense/. Acesso em: 22 de abr. 2019.

CAVALHEIRO, Renan. **Perícia Forense**: A profissão de Perito Digital está crescendo!.Mar. 2018 Disponível em: https://www.academiadeforensedigital.com.br/pericia-forense-perito-digital/.Acesso em:18 mai. 2019.

COELHO, Ana Carolina Assis. **Virtuais:** análise da prova. Disponível em: http://intertemas.toledoprudente.edu.br/ind.ex.php/Juridica/article/view/827/804, Acesso em: 22 abr. 2019.

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

COMPAIRED, Carlos Roman, SANTAGATI, Claudio Jesús. **Manual de Derecho Procesal Penal**. Buenos Aires: Juridicas, 2010.

CORREIA, Gustavo Testa. **Aspectos Jurídicos da Internet**. São Paulo: Editora Saraiva, 2000.

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

DA SILVA ALMEIDA, J.; Roque, B. V. S. **ChallengesOf The Law In The Regulation:** Of Legal Relations In Deep Web And Cyber Crimefigshare, 9 fev. 2018. Disponível em: https://figshare.com/articles/challenges_of_the_law_in_the_regulation_of_legal_relations_in_deep_web_and_cyber_crime/5873892/1. Acesso em: 29 mar. 2019.

DAOUN, Alexandre Jean; LIMA, Gisele Truzzi de. **Crimes Informáticos:** o Direito Penal na Era da Informação. Disponível em: http://www.truzzi.com.br/pdf/artigo-crimes-informaticos-gisele-truzzi-alexandre-daoun.pdf. Acesso em: 30 mai. 2018.

DEL PINO, Dr. Santiago**. Manual de Manejo de Evidencias Digitales y Entornos Informáticos.** Versión 2.0. s.n.

DIAS, Vera Marques. **A Problemática da Investigação do Cibercrime**. Data Venia, Revista Jurídica Digital, Ano 1, n.º 1, Julho-Dezembro 2012, ISSN 2182-8242.

DODGE, Raquel Elias Ferreira, **Crime por computador** - Ministério Público Federal - Brasil coord. e org. II. Título. Roteiro de atuação: crimes cibernéticos. 2 ed. rev. - Brasília: MPF/2ªCCR, 2013.

DULLIUS, Aladio Anastacio; HIPPLER, Aldair; FRANCO, Elisa Lunardi. **Dos Crimes Praticados em Ambientes Virtuais**. Santa Rosa, 2012. Disponível em: http://www.conteudojuridico.com.br/artigo,dos-crimes-praticados-em-ambientes-virtuais,38483.html. Acesso em: 14 abr. 2018.

E-GOV. 2004. **Diferença Entre *Hackers*, *Phreakers* e *Pirates*.**.Disponível em: http://www.egov.ufsc.br/portal/conteudo/saiba-diferen%C3%A7a-entre-hackers-crackers-white-hat-black-hat-gray-hat-entre-outros. Acesso em: 02 mai. 2018.

FBI.gov isanofficial site ofthe U.S. government, **U.S. Department of Justice**. Disponível em: https://www.fbi.gov/about-us/lab/forensic-sciencecommunications/fsc/april2000/swgde.htm/. Acesso em: 05 abr. 2019.

FERREIRA, Ivette Senise. **A Criminalidade Informática.** Direito e Internet - Aspectos Jurídicos Relevantes. Editora Edipro, 2011.

FERREIRA, Ivette Senise. **Direito & Internet:** Aspectos Jurídicos Relevantes. 2. ed. São Paulo: QuartierLatin , 2005.

FIGUEIREDO, Jonathan. **História da Internet**. 2013. Disponível em: jonathanfoste.blogspot.com/2013/08/historia-da-internet-acesso-internet.html. Acesso em: 29 abr.2019.

FIORILLO, Celso Antonio Pacheco. **Crimes no meio ambiente digital**. São Paulo: Saraiva, 2013.

FÓRUM DE GOVERNANÇA DA INTERNET [livro eletrônico]: relatórios dos dez primeiros anos do IGF / Núcleo de Informação e Coordenação do Ponto BR ; [tradução Linguagem Idiomas]. - São Paulo: **Comitê Gestor da Internet no Brasil**,

2017. -- (Cadernos CGI.br Referências) 6,95 Mb ; PDF Título original: IGFs' chairsummaries Vários colaboradores. Bibliografia. ISBN 978-85-5559-055-9. Disponível em: https://cgi.br/media/docs/publicacoes/1/CadernoCGIbr_Forum_de_Governanca_da_Internet.pdf. Acesso em 10 mai. 2019.

GANDINI, João Agnaldo Donizeti .SALOMÃO,Diana Paola da Silva e Jacob,Cristiane. Jul. 2016.**A Validade jurídica dos documentos digitais.** Disponível em: http://www.ambito-juridico.com.br/site/index.php?artigo_id=4411&n_link=revista_artigos_leitura. Acesso em:30 abr.2019.

GETNINJAS. **Tipos mais Comuns de Invasão de Computador**. Disponível em https://www.getninjas.com.br/guia/assistencia-tecnica/computador-desktop/os-tipos-mais-comuns-de-virus-de-computador/ Acesso em: 26 abr. 2018.

GOMES FILHO, Antônio Magalhães, Notas sobre a terminologia da prova.*In:* YARSHELL, Flávio Luiz; MORAES, Maurício Zanoide (Orgs.). **Estudos em homenagem à Professora Ada Pelegrine Grinover**. São Paulo: DPJ, 2005.

GRECO FILHO, Vicente**. Algumas observações sobre o direito penal e a internet**. Boletim do IBCCrim. São Paulo. Ed. Esp., ano 8, n. 95, out. 2000.

GRECO, Rogério. **Curso de Direito Penal** – Parte Geral. 4. ed. Rio de Janeiro: Impetus. 2004.

GRINOVER, Ada Pellegrini. **A Iniciativa Instrutória do Juiz no ProcessoPenal Acusatório.** Brasília, Revista Jurídica Consulex, nº. 169, Out. 2006.

HISTÓRIAZONE, Jul 14, 2016, **As ordálias da Idade Média, ou "o juízo de Deus.** Disponível em: https://historiazine.com/as-ordalias-da-idade-media-d090cbac4831. Acesso em 28 mar. 2019.

INFOPEDIA. 2006. **Cibercrime**. Disponível em: https://www.infopedia.pt/dicionarios/lingua-portuguesa/cibercrime. Acesso em: 09 abr.2018.

Internet FAQ Archives. **Guidelines for Evidence Collection and Archiving:** RFC 3227. Disponível em: http://www.faqs.org/rfcs/rfc3227.html, Acesso em 30 mar. 2019.

JESUS, Damásio Evangelista de. **Manual de Crimes Informáticos.** São Paulo: Saraiva, 2016.

KAMINSKI, Omar. 2010. **Tratado Internacional contra crimes na Internet.** Disponível em: https://www.conjur.com.br/2001-nov-24/convencao_lanca_tratado_internacional_cibercrimes#author. Acesso em: 24 ago. 2018.

KERSTEN, Vinicius Mendez. Ano 2017. **O Código de Hamurabi através de uma visão humanitária.** Disponível em: http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=4113 Acesso em: 28 mar. 2018.

LA CHAPELLE, Bertrand; FEHLINGER, Paul. **Jurisdiction on the internet:** from legal arms race to transnational cooperation. Internet &Jurisdiction paper. Abr. 2016. Disponível em: https://www.internetjurisdiction.net/uploads/pdfs/Papers/IJ-Paper-Jurisdiction-on-the-Internet-PDF.pdf. Acesso: 06 jan. 2019.

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

LOPES JR, Aury. **Direito Processual Penal e Sua Conformidade Constitucional.** 8. ed.Lumen Juris. Rio de Janeiro, 2011.

LOPES Jr. Aury,DA ROSA Alexandre Morais; BULHÕES Gabriel, **Investigação defensiva:** poder da advocacia e direito da cidadania. Disponível em: https://www.conjur.com.br/2019-fev-01/limite-penal-investigacao-defensiva-poder-dever-advocacia-direito-cidadania, Acesso em: 01 mar.2019.

LOPES JUNIOR, Aury. **Direito Processual Penal**. 10. ed. São Paulo: Saraiva, 2013.

LOPES, Petter. **Perícia Digital**.Forense Digital, Perícia Forense Computacional. Dez. 2013. Disponível em: https://periciacomputacional.com/pericia-digital/. Acesso em: 22 mar. 2019.

MACHADO, PATRÍCIA GOMES. **O Artigo 155 do CPP e os crimes de competência do júri.**Set. 2015. Disponível em: http://www.conteudojuridico.com.br/artigo,o-artigo-155-do-cpp-e-os-crimes-de-competencia-do-juri,54459.html. Acesso em: 22 abr. 2019.

MAGGIO, Vicente de Paula Rodrigues. **Novo crime**: invasão de dispositivo informático - Disponível em: https://vicentemaggio.jusbrasil.com.br/artigos/121942478/novo-crime-invasao-de-dispositivo-informatico-cp-art-154-a. Acesso em: 20 nov. 2018.

MALAQUIAS,Roberto Antônio Darós. **Crime Cibernético e Provas** - A investigação criminal em busca da verdade. Curitiba: Editora Juruá, 2012.

MANUSRTI- **Código de Manu** (200 A.C. e 200 D.C.). Disponível em: http://www.ufra.edu.br/legislacao/CODIGO%20DE%20MANU.pdf. Acesso em: 29 mar. 2018.

MARCONDES, José Sérgio.**Tecnologia de Identificação Aplicada no Controle de Acesso**. 2016. Disponível em: https://gestaodesegurancaprivada.com.br/tecnologias-de-identificacao/. Acesso em: 25 abr.2019.

MARINONI, Luiz Guilherme; MITIDIERO, Daniel**. Código de processo civil comentado.** 3ª ed.São Paulo: RT, 2011.

MORAIS, José Luiz Bolzan de; MENEZES NETO, Elias Jacob de. **Marco Civil da Internet**: A insuficiência do marco civil da internet na proteção das comunicações privadas armazenadas e do fluxo de dados a partir do paradigma da surveillance. Organizadores: George Salomão e Ronaldo Lemos. São Paulo: Atlas, 2014.

MOSSIM, Heráclito Antônio. **Compêndio de Processo Penal**. São Paulo: Manole, 2010.

NOVAIS, Rafael. **HD**: Entenda onde seus dados são armazenados. Mai.2015. Disponível em:https://www.psafe.com/blog/hd-entenda-onde-seus-dados-sao-armazenados/. Acesso em: 30 fev. 2019.

NUCCI, Guilherme de Souza, **O Valor da Confissão como meio de Prova no Processo Penal**, 2. ed., rev. E atual. São Paulo: Revista dos Tribunais, 1999.

NUCCI, Guilherme de Souza, **O Valor da Confissão como meio de Prova no Processo Penal**, 2. ed., rev. E atual. São Paulo: Revista dos Tribunais, 2015.

OLIVEIRA, Eugênio Pacellide.**Curso de processo Penal**. 13. ed. Rio de Janeiro: Lummen Juris, 2010.

OLIVEIRA, William César Pinto de. **Lei Carolina Dieckmann**. Disponível em: http://jus.com.br/revista/texto/23655. Acesso em: 12 jun. 2018.

PACHECO, Gisele Freitas – COSTA, Renato Lopes. **Crimes Virtuais e a Legislação Penal Brasileira.** Disponível em : http://fadipa.educacao.ws/ojs-2.3.3-3/index.php/cjuridicas/article/viewFile/269/pdf. Acesso em: 12 set. 2018.

PEREIRA, Leonardo. ***Deep web*****:** saiba o que acontece na parte obscura da internet. Olhar Digital, 2012. Disponível em: https://olhardigital.com.br/fique_seguro/noticia/deep-web-saiba-o-que-acontece-na-parte-obscura-da-internet/31120. Acesso em: 12 mar.2018.

PERLINGIERI, Pietro. **O Direito Civil na Legalidade Constitucional.** Trad. Maria Cristina de Cicco. Rio de Janeiro. Ed. Renovar, 2008.

PINHEIRO, Patrícia Peck. **Direito Digital**. São Paulo: Editora Saraiva, 2013.

PINHEIRO, Patrícia Peck; HAIKAL, Victor Auilo. **A nova lei de crimes digitais**. 2013. Disponível em: www.pppadvogados.com.br/Publicacoes.aspx?v=1&nid=1432. Acesso em: 23 mar. 2019.

PROJETO DE LEI ANTICRIME. **Anteprojeto de Lei Nº , de 2019**. Disponível em https://www.justica.gov.br/news/collective-nitf-content-1549284631.06/projeto-de-lei-anticrime.pdf. Acesso em 16 mai. 2019.

RANGEL, Paulo. **Direito Processual Penal**. 20. ed. São Paulo: Atlas, 2012.

RANGEL, Paulo. **Direito Processual Penal**. Rio de Janeiro. Lumen Juris, 2003.

Revista Jurídica Digital, Ano 1, n.º 1, Julho-Dezembro 2012, ISSN 2182-8242.

ROCHA,Manuel Lopes**;** GAMA Filho, Remy. **Crimes da Informática**. Editora: CopyMarket. 2000.

RODOTÀ, Stefano. **A vida na sociedade da vigilância** - a privacidade hoje. Rio de Janeiro: Renovar, 2008. Tradução de: Danilo Doneda, Luciana Cabral Doneda.

RODRIGUES, Benjamim Silva. **Direito Penal Parte Especial**.Tomo I, Direito Penal Informático-Digital, Contributo para a Fundamentação da sua Autonomia Dogmática e Científica à Luz do novo Paradigma de Investigação Criminal: a Ciência Forense Digital e a Prova Digital. Coimbra Editora, Limitada. ISBN: 978-989-95779-5-4.

ROSSINI, Augusto Eduardo de Souza**. Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

SIGNIFICADOS.com.br. Disponível em: https://www.significados.com.br/portugues/. Acesso em: 20 mar. 2019. Ás 15h42.

SILVA, Ricardo José de Souza.**Delito Virtual**: Um diálogo sobre as transgressões online do mundo real. Delictæ: Revista de Estudos Interdisciplinares sobre o Delito. Volume 2. Número 4. Jan.- Jun./2018 Belo Horizonte: Centro de Investigações Interdisciplinares sobre o Delito, 2018. Semestral. ISSN: 2526-5180 (eletrônico). Direito – II. Periódicos – III. Brasil.

SILVA. Patrícia Santos da. **Direito e Crime Cibernético**: análise da competência em razão do lugar no julgamento de ações penais [recurso eletrônico] . Brasília, Ed. Vestnik, 2015. sn.

STRAZZI, Alessandra. **Crimes contra a honra** - diferenças entre calúnia, difamação e injúria, Disponível em : https://alestrazzi.jusbrasil.com.br/artigos/130177918/crimes-contra-a-honra-diferencas-entre-calunia-difamacao-e-injuria. Acesso em: 28 jun. 2018.

TALAMINI, Eduardo. Mar. 2016. **Produção antecipada de prova**.Disponível em: https://www.migalhas.com.br/dePeso/16,MI235462,51045-Producao+antecipada+de+prova. Acesso em: 22 mar. 2019.

TANENBAUM, Andrew S. **Redes de Computadores.** Brasil.Editora**,**Elsevier. 2003.

TAVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Curso de Direito Processual Penal**. Salvador: Jus Podivm, 2014.

TOLEDO, Francisco de Assis. **Princípios Básicos de Direito Penal**. São Paulo: Ed. Saraiva, 1991.

TOURINHO FILHO, Fernando da Costa. **Processo Penal**. São Paulo: 2005.

VERDELHO, Pedro. **Cibercrime e segurança informática**, Polícia e Justiça, série 3, n. 6 jul/dez..2005.

VIANA, Marco Túlio, **Fundamentos de direito penal informático.** Do acesso não autorizado a sistemas computacionais**.** Rio de Janeiro: Forense, 2003.

WAZLAWICK, Raul, **História da Computação.** Brasil. Editora: Elsevier. 2016.

WELCH, Thomas. Computer Crime Investigationand Computer Forensics. *In*: TIPTON, Harold; KRAUSE, Micki (Org.). **Information Security Management Handbook.** 6th ed. Florida: Auerbach Publications, 2007.