UNIVERSIDADE ESTADUAL DO PIAUÍ – UESPI
Centro De Ciências Sociais Aplicadas - CCSA
Curso de bacharelado em Direito

André Lucas Coimbra França

OS CRIMES PRATICADOS PELO COMPUTADOR:
dificuldade de apuração dos fatos

Teresina
2017

André Lucas Coimbra França

OS CRIMES PRATICADOS PELO COMPUTADOR:
dificuldade de apuração dos fatos

Monografia apresentada à coordenação do curso de bacharelado em Direito da Universidade Estadual do Piauí – UESPI, como requisito parcial para a obtenção do título de Bacharel em Direito.

Orientador (a): Profª. Ma. Maria dos Remédios Lima do Nascimento

Teresina

2017

F814c França, André Lucas Coimbra.
Os crimes praticados pelo computador: dificuldade de apuração dos fatos / André Lucas Coimbra França. - 2017.
59 f.

Monografia (graduação) – Universidade Estadual do Piauí - UESPI, *Campus* Torquato Neto, Curso de Bacharelado em Direito, 2017.
"Orientador: Profª. Ma. Maria dos Remédios Lima do Nascimento."

1. Internet. 2. Crimes Virtuais. 3. Crimes Virtuais – Provas. 4. Crimes Virtuais – Autoria. 5. Crimes Virtuais – Apuração dos Fatos. I. Título.

CDD: 340

Ficha elaborada pelo Serviço de Catalogação da Universidade Estadual do Piauí – UESPI Ana Angélica P. Teixeira (Bibliotecária) CRB 3ª /1217

André Lucas Coimbra França

OS CRIMES PRATICADOS PELO COMPUTADOR:

dificuldade de apuração dos fatos

Monografia apresentada à coordenação do curso de bacharelado em Direito da Universidade Estadual do Piauí – UESPI, como requisito parcial para a obtenção do título de Bacharel em Direito.

Monografia aprovada em ___/___/_____

BANCA EXAMINADORA

_____

Profª. Ma. Maria dos Remédios Lima do Nascimento

Orientadora

_____

Prof. Jhon Kennedy Teixeira Lisbino

UESPI

_____

Prof. Elvis Gomes Marques Filho

UESPI

RESUMO

O crescimento da Internet e o desenvolvimento tecnológico possibilitaram a ocorrência de uma nova modalidade de crimes: os crimes virtuais ou cybercrimes. Levando em consideração o surgimento desses novos delitos pelo uso da internet e a necessidade do Direito acompanhar as mudanças resultantes dos avanços tecnológicos, pois estas interferem nos aspectos jurídicos, optou-se por abordar esse tema. Os crimes praticados pelo computador serão discutidos sob a ótica da Informática no Direito Penal e a necessidade de adaptação dos textos legais com a realidade da sociedade. A Lei 12.737/12, ou Lei “ Carolina Dieckmann”, foi o primeiro passo dado no combate a esses crimes. Entretanto, além da tipificação dos novos delitos decorrentes da influência dos avanços tecnológicos na sociedade atual, outras questões, estreitamente ligadas a algumas características inerentes aos crimes cibernéticos, merecem uma atenção especial. A forma que se dão esses delitos, com bastante velocidade e de forma anônima, assim como os bens jurídicos atingidos por eles, são peculiaridades que dificultam a investigação criminal e a produção de provas. A necessidade de peritos especializados, a dificuldade na identificação da autoria e a necessidade da produção antecipada de provas são as questões objeto de análise do presente trabalho.

Palavras-chave: Internet. Crimes virtuais. Provas. Autoria. Apuração dos fatos.

ABSTRACT

The growth of the Internet and technological development have enabled a new type of crime to occur: virtual crimes or cybercrimes. Taking into account the emergence of these new crimes for the use of the Internet and the need for Law to accompany the changes resulting from technological advances, as these interfere in the legal aspects, it was decided to approach this issue. The crimes practiced by the computer will be discussed from the point of view of Informatics in Criminal Law and the need to adapt legal texts to the reality of society. The Law 12.737 / 12, or "Carolina Dieckmann" Act, was the first step taken in combating these crimes. However, in addition to the typification of new offenses arising from the influence of technological advances in today's society, other issues, closely linked to some characteristics inherent in cybercrime, deserve special attention. The manner in which these crimes occur, with a great deal of speed and anonymity, as well as the juridical assets which they incurred, are peculiarities that hinder criminal investigation and the production of evidence. The need for specialized experts, the difficulty in identifying the authorship and the need for the anticipated production of evidence are the issues that are the object of the present study.

Key words: Internet. Virtual crimes. Evidence. Authorship. Fact finding.

LISTA DE ABREVIATURA E SIGLAS

Art.	Artigo
CRFB	Constituição da República Federativa do Brasil
CP	Código Penal
ECA	Estatuto da Criança e do Adolescente
FAPESP	Fundação do Amparo à Pesquisa no Estado de São Paulo
INT	Instituto Nacional de Tecnologia
IP	Internet Protocol
MIT	Instituto de Tecnologia de Massachussets
PC	Personal Computer
TJ	TRIBUNAL DE JUSTIÇA
WWW	World Wide Web

SUMÁRIO

1 INTRODUÇÃO

A sociedade contemporânea tem passado por várias transformações ao longo do desenvolvimento das tecnologias de informação. Esse avanço tecnológico permitiu o surgimento da Internet, antes criada com o fim de comunicação meramente militar, que se popularizou e passou a abarcar a interligação de vários computadores ao redor do mundo proporcionando uma maior facilidade de comunicação.

Entretanto, com os benefícios desse meio de comunicação, não se pode olvidar das mazelas que ele também proporciona. As práticas de condutas ilícitas a cada ano ficam mais perigosas na medida que as tecnologias se renovam. A internet se tornou um ambiente propício para o cometimento de vários crimes, sejam aqueles que passaram recentemente a serem tipificados e aqueles que já o eram e encontravam no ambiente cibernético só mais uma forma de serem praticados.

O presente trabalho tem o objetivo principal de analisar a investigação dos crimes de internet e a dificuldade que se se confere à apuração dos fatos que ensejam a realização de tais delitos. Devido ao avanço tecnológico, estes crimes vêm sendo configurados não de forma pessoal, mas sim de forma anônima através do uso da rede de computadores. Este anonimato faz com que as pessoas tenham a ilusão de uma segurança muito fragilizada, uma vez que, toda máquina ao conectar-se na rede mundial de computares, a mesma obtém um endereçamento no qual permite que haja uma comunicação sem conflitos e choque de transmissão de dados. Este endereço consiste no chamado IP (Internet Protocol), que é responsável pela transmissão e receptação de dados entre as demais máquinas sem que tenha perda de informação.

Isso se dá pela distribuição de servidores que identificam cada máquina conectada à internet, permitindo uma comunicação de forma estável sem o choque e a perda dessas informações.

Com a identificação possível de cada máquina na rede, os usuários de cada uma delas estão seguramente identificados nos servidores, onde os mesmos armazenam a localidade e o usuário que ali está conectado, possibilitando assim que se chegue àqueles usuários que por ventura usem a internet para a prática dos crimes contra a honra e entre outros crimes, que podem ser realizados através da rede.

O objetivo deste estudo é focar nos crimes de internet identificando como os mesmos ocorrem e onde se configuram os eventuais delitos, como também a possibilidade de se chegar ao autor para que haja o enquadramento dele nas normas que estão tipificadas no nosso ordenamento jurídico.

Também se discutirá a problemática na obtenção das provas e a fragilidade que estas têm devido à facilidade de perda definitiva das mesmas, pelas características de sua virtualização.

Buscar-se-á esclarecer os pontos conflitantes na interpretação na quebra do sigilo do IP, uma vez que este endereçamento não tem características sigilosas, pois trata apenas de um dado no qual permite a comunicação da máquina e não o anonimato da mesma, e poderá se demonstrar facilmente que um usuário que tenha conhecimentos na informática pode obtê-lo facilmente.

Com este aprofundamento buscar-se-á trazer ao nosso ordenamento mais celeridade na obtenção das provas e a punição dos autores que materializarem esses delitos na rede.

2 CRIMES PRATICADOS POR MEIO DO COMPUTADOR E O DIREITO PENAL BRASILEIRO

Quando se fala dos crimes praticados por meio do computador tem-se a ideia dos delitos cometidos contra ele ou através dele. Grande parte destas infrações são realizadas pela internet, que é o meio de comunicação mais utilizado na contemporaneidade. Define Lima (2014):

> Referidos crimes podem ser conceituados como condutas de acesso não autorizados pelos sistemas informáticos e são considerados como ações destrutivas, no qual, podemos citar como exemplo as interceptações de comunicação, modificações de dados, infrações de direitos autorais, incitação ao ódio e descriminação, escárnio religioso, difusão de pornografia infantil, terrorismo, entre outros.

Tais crimes podem receber diversas denominações, não havendo um consenso sobre a melhor denominação para estes delitos que estão ligados ao uso da tecnologia. Crimes de computação, delitos de informática, abuso de computador, fraude informática e, mesmo assim, tais conceitos não abrangem ainda todas as más condutas ligadas à tecnologia. Portanto, deve-se ficar atento quando se conceitua o crime, tendo em vista a diversidade e complexidade de situações no ambiente virtual. (LIMA, 2014)

Portanto, ao analisar um crime de informática, deve-se analisar se o mesmo é crime de internet ou não para depois ser aplicado o tipo penal correspondente à infração, visando a proteção do bem jurídico exposto ao risco.

Com certa dedicação é possível classificar e constatar um crime virtual visto que não é uma tarefa simples e devido a poucas conclusões a esse respeito. Ano após ano as tecnologias evoluem e as opiniões dos estudiosos também.

Para Lima (2014) “Existem condutas que utilizam os computadores como meio para o cometimento dos delitos e há casos em que sem o uso do sistema informático não seria possível a consumação de certos tipos penais. ”

Isso quer dizer que há crimes já previstos na legislação penal que não diferem na tipicidade se forem cometidos virtualmente. Não há muitas dificuldades quanto a

isso, mas a forma de sua execução foi inovada. O computador é “mero” instrumento do crime.

Nestes tipos de crimes estão incluídas todas as espécies de infrações previstas nas leis penais que são praticados por meio eletrônico. A novidade se dá pelo *modus operandi*, assim não se admitindo a criação de novos dispositivos legais para o que já está tutelado em matéria penal. É o que ocorre com os crimes de injúria, calúnia, difamação, estelionato, plágio e até mesmo furto. São classificados como os “crimes de informática impróprios”.

Já as violações contra o sistema de informática atingem bens antes não tutelados pelo legislador penal, como dados, informações*, sites*, *home pages, e-mail* etc. A dificuldade é muito grande pelo fato de serem bens que ainda não gozam de proteção plena. O computador é usado tanto como meio para atingi-los quanto fim destas práticas delituosas.

“Portanto, não há que se falar em crime relativamente àquelas condutas que ainda não foram previstas pelo legislador como fato típico e, desta maneira, o autor não poderá ser punido nem compelido a deixar de praticá-las. ” (NETO, 2009).

Entretanto, em novembro de 2012, foi criada a Lei nº 12.737 que dispõe sobre a tipificação criminal de delitos informáticos. Este instituto adicionou os artigos 154-A e 154-B e passou punir os responsáveis pelos “crimes de informática próprios” caso praticassem algum ato que atentasse contra o sistema de informações, como invasão de dispositivo informático, adulteração e destruição de dados etc.

Costa (1995), na década de 90, onde era raro o uso deste meio de comunicação pela população, já afirmava que ocorreriam várias destas práticas no Brasil e, mesmo assim, não seriam noticiadas para evitar o abalo da credibilidade das empresas, por se pensar que a própria divulgação fosse pior que o resultado da própria ação. Isso acarretaria desespero, comoção geral e perda de vários clientes que poderiam se recusar a negociar com uma empresa por ela não ter segurança nos seus dados, informações e sistemas.

O nosso Código Penal, quando defrontado com delitos dessa natureza, deixa claras as suas deficiências com relação ao tema, até porque a Parte Especial do referido Código data de 1940, época em que os sistemas computadorizados ainda não tinham aportado em nosso país (PIRAGIBE, 1985). Segundo Ferreira (2009):

> [...]verifica-se a “quase” impossibilidade de se aplicar esta parte do Código aos chamados “Crimes de Informática”. Porém, através dos princípios gerais do Direito Penal, é possível aplicar regras da Parte Geral do Código Penal a esse tipo de conduta.

Segundo Costa (1995, apud FERREIRA, 2009) os crimes de informática “[...] devem ser classificados adequadamente para que o legislador pátrio possa elaborar normas eficientes, e, se necessário, indicar as normas vigentes que podem ser aplicadas, porém é imprescindível o estudo crítico desses delitos. ” Deve ser feita uma individualização de suas espécies para que haja um aprofundamento do objeto jurídico a ser tutelado sem prejuízo da aplicação da norma e da pena adequadas ao delito.

A seguir será explorado o histórico do computador, da Internet e dos crimes de Internet para um maior esclarecimento e aprofundamento do assunto.

2.1 Histórico

2.1.1 História do Computador

Para Castro (2003, p.1):

> Computador é conceituado como sendo um processador de dados que pode efetuar cálculos importantes, incluindo numerosas operações aritméticas e lógicas, sem a intervenção do operador humano durante a execução. É a máquina ou sistema que armazena e transforma informações, sob o controle de instruções predeterminadas. Normalmente consiste em equipamento de entrada e saída, equipamento de armazenamento ou memória, unidade aritmética e lógica e unidade de controle. Em um último sentido, pode ser considerado como uma máquina que manipula informações sob diversas formas, podendo receber, comunicar, arquivar e recuperar dados digitais ou analógicos, bem como efetuar operações sobre lei.

O computador é uma máquina complexa, criado inicialmente sob o intuito de fazer cálculos muito complexos e salvar grande quantidade de tempo. A primeira máquina que possuía estas características foi criada no período da Renascença, e conforme explicam Muoio e Aguiar (2006, p.230):

> Através dos tempos, um grande número de cientistas pesquisou a possibilidade de se criar uma máquina para se operar os cálculos. Como

> resultado disso, a primeira calculadora, do modo como hoje conhecemos, surgiu na Renascença, criada por Wilhelm Schickard (1592 - 1635). Tratava-se de uma máquina que operava soma, subtração, multiplicação e divisão, mas que foi perdida durante a Guerra dos Trinta Anos. E o seu inventor faleceu, acometida pela peste, sem ter podido defender sua criação. Deste modo, atribui-se geralmente a Blaise Pascal (1623 – 1662) a construção da primeira calculadora. Porém, sua PASCALINE somente fazia somas e subtrações.

Com o passar dos anos, este tipo de máquina foi se modernizando e passou a ser um tear mecânico que funcionava através de instruções contidas em cartões perfurados.

> Era preciso criar uma forma de “ler” instruções, aprimorar um dispositivo de “entrada”. Isto só veio a ser solucionado em 1801, durante a Revolução Industrial, quando o cientista francês Joseph Marie Jacquard inventou um tear mecânico com uma leitora de cartões automática, que lia cartões perfurados, transformando um desenho abstrato num padrão de cores, determinado através de voltas de cada fio colorido no lugar certo. A máquina de Jacquard trabalhava tão bem que milhares de tecelões desempregados se revoltaram e quase mataram o inventor. (MUOIO; AGUIAR, 2006, p. 231)

A partir desta ideia, foi facilitado a Charles Babbage a construção de novas máquinas que faziam cálculos:

> Com a ideia do cartão perfurado de Jacquard, Babbage criou então o “calculador analítico”, a estrutura básica de um computador como o conhecemos atualmente. Entre os seus componentes estava o “moinho”, uma roda dentada que se encontrava no coração da máquina e que seria uma enorme mastigadora de números, uma máquina de somar com precisão de 50 casas decimais. As “instruções” seriam lidas em cartões perfurados, isto é, os cartões perfurados transportariam não só os números, mas o padrão de moagem também. Portanto, a máquina precisaria de um dispositivo de ENTRADA para ler os cartões. Babbage idealizou uma unidade de memória ou “armazém” para guardar os números para referências futuras. Esta unidade seria um banco de 1000 “registradores”, cada um deles capaz de armazenar um número de 50 dígitos. Estes números poderiam ser ou um número dado nos cartões de entrada ou o resultado das operações do moinho. E finalmente a SAÍDA: Babbage desenhou a primeira máquina automática de impressão para mostrar o resultado dos cálculos. (MUOIO; AGUIAR, 2006, p. 231)

Em 1946 se deu o marco da criação do primeiro computador eletrônico com fins militares, o ENIAC. Explica Castro (2003, p. 2):

> O primeiro computador eletrônico data de 1946 e foi criado pelas necessidades militares. Denominou-se ENIAC – Eletronic Numeric Integrator and Calculator e foi utilizado para montar tabelas de cálculo das

> trajetórias dos projéteis. Em 1951 apareceram os primeiros computadores em série e, com a rápida e avassaladora evolução tecnológica, temos hoje os PC (computadores pessoais) e notebooks.

Com isso, percebe-se como se deu o processo “evolutivo” do computador até chegar a esta máquina tão complexa que é usada tanto como instrumento para crimes quanto objeto deles.

2.1.2 História da Internet

É inegável o papel tão importante da Internet no dia a dia da população de qualquer região do mundo. Esta grande rede se fixou tanto na dinâmica do mundo contemporâneo que hoje é indispensável, seja para comunicação, segurança ou ferramenta de trabalho. Afirma Castro (2003, p.3):

> Internet é uma grande rede de comunicação mundial, onde estão interligados milhões de computadores, sejam eles universitários, militares, comerciais, científicos ou pessoais, todos interconectados. É uma rede de redes, que pode ser conectada por linhas telefônicas, satélites, ligações por microondas ou por fibra ótica.

Percebe-se que é uma tecnologia em que o usuário tem controle sobre seu conteúdo, onde o mesmo pode buscar informações daquilo que satisfaça suas necessidades e que seja de seu interesse. Conforme explica Fontes (2006, p.73):

> A Internet é uma nova forma de acessar informações. Apesar de ter se tornado comercial apenas nos meados dos anos 1990, sem sombra de dúvida, a Internet já contém uma quantidade muito grande de informações de divertimento, de pesquisa, de educação e de assuntos profissionais. Da mesma forma que consultamos jornais e revistas, a Internet permite que tenhamos acesso a essas mesmas informações de maneira mais rápida.

Inicialmente se achava que a criação da Internet tinha propósito unicamente militar, para comunicação entre bases militares. Mas, conforme o pensamento de Finkelstein (2008, p.407), não era bem assim:

> Sua predecessora chamava-se ARPANET, tendo sido desenvolvida em 1969. Sem dúvida há boatos de que a ARPANET foi desenvolvida para fins militares, mas a tese dominante é a de que a Internet surgiu com o objetivo de pesquisa de um projeto da agência norte-americana ARPA. A conexão teve início ao interligarem-se os computadores de quatro universidades, passando, a partir disso, a ser conhecida como ARPANET. Em 1970, esse projeto foi intensamente estudado por pesquisadores, o que resultou na concepção de um conjunto de protocolos que é a base da Internet. Depois,

> o ARPA integrou redes de computadores de vários centros de pesquisa. Em 1986, a NSFNET, da entidade americana NSF, interligou-se a ARPANET, o que deu finalmente origem às bases da atual Internet.

A Internet, como é conhecida hoje, só foi formada em 1989 com o surgimento da *World Wide Web* (WWW). Tal surgimento facilitou e popularizou seu uso diante da busca por informações (CASTRO, 2004).

Já no Brasil, a Internet surgiu como uma forma de interligar as universidades brasileiras com as universidades de fora do país, numa mútua troca de informações entre elas.

> Foi em 1988 que a Internet finalmente chegou ao Brasil. Ela foi apresentada por estudantes de cursos nos Estados Unidos que, ao retornar ao Brasil, sentiam a falta de intercâmbio mantido no exterior com outras instituições científicas. Foi assim que a Fundação do Amparo à Pesquisa no Estado de São Paulo (FAPESP), ligada à Secretaria Estadual de Ciência e Tecnologia, iniciou diversos contatos e que a troca de dados começou a ser feita. O serviço foi inaugurado, oficialmente, em abril de 1989. (FINKELSTEIN, 2008, p.408)

2.1.3 História dos Crimes de Informática

Para se ter uma ideia dos Crimes de Informática, deve-se perceber de qual forma estes tais delitos tiveram seu início e como se propagaram. A partir de uma análise breve do histórico será delimitado os tipos de crimes e como eles acontecem.

> Em novembro de 1961, desenvolvedores do MIT (Instituto de Tecnologia de Massachussets) demonstravam o seu sistema experimental compatível com gerenciamento de tempo, o que permitia quatro usuários trabalhando em terminais rodar programas de outros usuários. No final dos anos 60, terminais conectados por modem poderiam ser facilmente invadidos, já que, na época, ninguém se preocupava em colocar senhas. (ASSUNÇÃO, 2008)

Isso quer dizer que mesmo antes da criação da Internet já haviam práticas que hoje poderiam ser consideradas como Crimes de Informática. Porém, Ferreira (2005, p.239) afirmava que os crimes virtuais se iniciaram na década de 60 e só na década seguinte foram realizados os exames criminológicos:

> [...] o surgimento dessa espécie de criminalidade remonta à década de 1960, época em que aparecem na imprensa e na literatura científica os primeiros casos do uso do computador para a prática de delitos, constituídos sobretudo por manipulações, sabotagens, espionagem e uso

> abusivo de computadores e sistemas, denunciados sobretudo em matérias jornalísticas. Somente na década seguinte é que iriam iniciar-se os estudos sistemáticos e científicos sobre essa matéria, com o emprego de métodos criminológicos, analisando-se um limitado número de delitos informáticos que haviam sido denunciados, entre os quais alguns casos de grande repercussão na Europa por envolverem empresas de renome mundial, sabendo-se, porém, da existência de uma grande cifra negra não considerada nas estatísticas. (FERREIRA, 2005, P.239)

A partir dos anos 80 estas práticas começaram a variar e se intensificar com a expansão das práticas criminosas de manipulação de caixas bancárias, pirataria de programas de computador, abusos nas telecomunicações, etc., revelando a vulnerabilidade desses sistemas e a necessidade imediata de segurança e de novas formas de controle e incriminação das condutas lesivas. (FERREIRA, 2005).

Assim, houve uma ampliação do conceito de crime informático, que começou a englobar crimes de natureza econômica, contra a intimidade e a vida privada, contra a propriedade intelectual, etc. Atualmente, com a popularização da Internet, constata-se o aumento de novas práticas delituosas, tais como a transferência eletrônica de fundos (*Internet banking*), intromissão abusiva em sistemas (hacking), disseminação de “vírus” em computadores, revelando a vulnerabilidade do sistema e a necessidade de prevenção destes delitos.

No ano de 1986 foi criada a primeira lei penal específica para os crimes de informática nos Estados Unidos. A lei foi chamada de Lei de Fraude e Abuso de Computadores, onde em 1988 foi realizada a primeira prisão pela prática de um delito virtual. Robbert Tappan Morris Junior foi condenado a cinco anos de cadeia pela disseminação de um vírus de computador, atingindo mais de 50.000 máquinas (NETO, 2009).

Se verificou a importância da criação de uma lei que trata diretamente do resguardo aos bens jurídicos atingidos pela prática dos crimes cometidos pelo computador ou contra o computador. Dessa forma, se dá a segurança necessária às informações e às pessoas que estão “atrás” da máquina, mesmo que, para a apuração dos crimes, haja certa dificuldade.

O primeiro caso conhecido de crime de informática ocorrido no Brasil ocorreu em 1997 quando uma jornalista passou a receber diversos *e-mails* de cunho erótico-sexual, juntamente com mensagens de ameaça a sua integridade física. Se chegou ao responsável pelo delito e este teve que prestar serviços junto a Academia da Policia Civil, dando aula de informática para novos policiais. (NOGUEIRA, 2008).

Tais crimes são caracterizados pela repercussão e pela dificuldade no combate a eles, já que muitos autores se aproveitam do anonimato e ficam impunes enquanto a polícia investiga e tenta localizá-los.

2.2 Dos Crimes de Informática

Como já explicado anteriormente, os Crimes de Informática são toda e qualquer conduta ilegal ou prejudicial à sociedade que se realiza pelo uso de um computador. Além disso, podem receber várias denominações como “crimes de computador”, “cybercrimes”, “delitos de informática”, “delitos cibernéticos”, “infocrimes”, etc.

Para Ferreira (2005) as várias possibilidades de ação criminosa na área informática originaram uma forma de criminalidade que pode ser identificada pelo seu objeto ou meios de ação.

Daoun e Lima (20--, p.4, apud NETO, 2009) apresentam um conceito deste tipo de crime que está ligado a denominação dada pela doutrina penal, assim como nos tribunais brasileiros e na Organização para Cooperação Econômica e Desenvolvimento das Organizações das Nações Unidas:

> Pode-se afirmar que a doutrina penal e os tribunais brasileiros tem 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 a 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 dedados e/ou transmissão de dados.

Depreende-se que estes crimes atentam contra dados, sejam estes armazenados, compilados, transmissíveis ou em transmissão e os sistemas de informação. Para Ferreira (2009) existem dois elementos indissolúveis: dados, que é o objeto material, e *hardware,* que é a parte física do sistema, em conjunto com o *software*, que é a parte lógica do sistema, para realizar alguma conduta usando esses dados.

O Código Penal Brasileiro ainda carece de positivação de algumas condutas que se encaixam neste tipo de delito. Entretanto, com o advento da Lei 12.732/2012, tornou crime a invasão de aparelhos eletrônicos para obtenção de dados

particulares. Ela pretendeu estabelecer punições específicas para os crimes cibernéticos ao acrescentar artigos ao Código Penal, impondo prisões e multa a quem invadir computadores.

Porém, muitos juristas e criminalistas apontam irregularidades nessa lei citando falhas na qualidade técnica de sua redação, sem muitas discussões em torno do tema, o que deixa pontos em aberto. Há a ausência de definição de diversos termos técnicos inseridos na lei, o que inviabiliza a aplicação do tipo penal. O texto legal somente contempla as figuras típicas e não disciplina os meios processuais que garantem a eficácia da norma.

Recentemente, no dia 21 de fevereiro de 2017, foi aprovado o Projeto de Lei 5.555/13 (Lei Rose Leonel) na Câmara dos Deputados que propõe alterações na Lei 11.340/06 (Lei Maria da Penha) e no Código Penal (lei 2.848/40).

O texto do projeto de lei propõe a inclusão do inciso VI no art. 7° da lei 11.340/06, visando definir a Disseminação Indevida de Material Íntimo (DIMI) como forma de violência doméstica e familiar:

> Art. 7º São formas de violência doméstica e familiar contra a mulher, entre outras:
> ...
> VI – a violação da intimidade da mulher, a violação da intimidade da mulher, entendida como a divulgação, por meio da internet ou outro meio de propagação de informações, de dados pessoais, vídeos, áudios, montagens e fotocomposições da mulher, obtidos no âmbito das relações domésticas, de coabitação ou hospitalidade, sem seu expresso consentimento.

Portanto, torna crime a vingança virtual com a divulgação e a exposição pública da intimidade sexual, principalmente da mulher.

Pelo projeto, o Código Penal passa a conter o crime de exposição pública da intimidade sexual no capítulo que trata de injúria com ofensa à dignidade e ao decoro. O projeto deixa explícito como crime divulgar "através de imagem, vídeo ou qualquer outro meio, material que contenha cena de nudez ou de ato sexual de caráter privado". Se o crime for cometido por motivo torpe ou contra pessoa com deficiência, a pena de prisão do divulgador original da imagem será aumentada em um terço ou até mesmo metade.

Não obstante, ocorreu em agosto de 2017 a primeira prisão por estupro virtual no Brasil, exatamente no Estado do Piauí. Um homem chantageou e exigiu que uma

mulher lhe enviasse fotos praticando ato libidinoso consigo mesma, por meio da internet.

O tipo penal que o acusado terá de responder é o mesmo do estupro. O delegado que investigou o caso inclusive afirma que é o mesmo crime, em que uma pessoa obrigou outra por meio de ameaça a fazer ato libidinoso.

Como na maioria dos casos, o acusado e a vítima tiveram relacionamento por um período, quando ele tirou fotos da mulher nua enquanto dormia. Depois da separação, o homem criou perfis falsos em redes sociais e passou exigir que a ex-companheira enviasse fotos se masturbando — caso contrário, divulgaria as fotos que já tinha dela.

Para não ter suas fotos vazadas, a mulher atendeu a ordem. Porém, a extorsão continuou, com mais pedidos. Ela, ainda sem saber quem era que a ameaçava, buscou ajuda na polícia. As autoridades rastrearam o IP do técnico de informática e o prenderam.

Mesmo que não houve contato físico entre a vítima e o agressor, aquela foi ameaçada, constrangida mediante grave ameaça para manter ato libidinoso. Por isso, pode ser considerado um estupro ocorrido em ambiente virtual.

Rosa (2005, apud FERREIRA, 2009) destaca que existe um problema relacionado à dicotomização do delito comum e o de Informática, já que muitos doutrinadores garantem que não existem delitos dessa natureza, pois argumentam que os crimes cometidos com o computador encontram-se todos positivados na legislação brasileira. Porém, o autor destaca que existem crimes comuns – os previstos no Código Penal (CP) brasileiro, crimes comuns cometidos com o auxílio do computador - que encontram aplicação na legislação penal brasileira, visto que se enquadram nas condutas descritas nos tipos penais previstos no CP, e certas condutas que não estão tipificadas em tal legislação e que necessitam da utilização do computador para o resultado desejado. Esses são os “crimes de Informática” propriamente ditos e são essas situações que necessitam de um cuidado maior específico mesmo com o advento da lei que tipificou esses delitos.

2.3 Classificação dos Crimes de Informática

Diante da variedade de delitos cometidos no ambiente virtual, é necessário um estudo da classificação destes tipos de delitos. Existem várias classificações doutrinárias a respeito do tema que é amplamente discutido pelos autores.

Jorge e Wendt (2012, apud TATEOKI, 2016) afirmam que existem as ações prejudiciais atípicas e os crimes cibernéticos. As ações prejudiciais atípicas são aquelas condutas que causam prejuízo para a vítima através do uso da rede de computadores, mas não estão tipificados em lei. Por outro lado, os crimes cibernéticos se dividem em “crimes cibernéticos abertos” e “crimes exclusivamente cibernéticos”. Estes precisam necessariamente do meio da informática para cometer tal crime (crime de invasão de dispositivo informático, artigos 154-A e 154-B do Código Penal, introduzidos pela Lei 12.735/2012). Aqueles podem ou não ser praticados pelo meio informático, como no crime de violação de direito do autor.

Outra parte da doutrina entende que os crimes virtuais podem ser estudados levando-se em consideração o papel desempenhado pelo computador no contexto da prática do ato ilícito. O computador pode ser o alvo do ilícito (crime de invasão, contaminação por vírus, sabotagem do sistema, destruição ou modificação de conteúdo do banco de dados, furto de informação, furto de propriedade intelectual, vandalismo cibernético, acesso abusivo por funcionário, acesso abusivo por terceirizados, acesso abusivo por fora da empresa); pode ser o instrumento para o crime (crime de fraude em conta corrente e/ou cartões de crédito, transferência de valores ou alterações de saldos e fraude de telecomunicações, divulgação ou exploração de pornografia); pode ser incidental para outro crime (crimes contra honra, jogo ilegal, lavagem de dinheiro, fraudes contábeis, registro de atividades do crime organizado); e o crime pode estar associado com o computador (pirataria de software, falsificações de programas, divulgação, utilização ou reprodução ilícita de dados e programas de comércio ilegal de equipamentos e programas). (FERREIRA, 2001 apud TATEOKI, 2016)

Para Teixeira (2014 apud TATEOKI, 2016), existem os crimes de informática puros, mistos e comuns:

> [...] o primeiro são aqueles em que o sujeito visa especialmente o sistema de informática; as ações materializam, por exemplo, por atos de vandalismo contra a integridade do sistema ou pelo acesso desautorizado ao computador. Crime de informática misto se consubstancia nas ações em que o agente visa o bem juridicamente protegido diverso da informática, porém o sistema de informática é ferramenta imprescindível. E os crimes de

> informática comum são condutas em que agente utiliza o sistema de informática como mera ferramenta, não essencial à consumação do delito.

Já para Viana e Machado (2013 apud TATEOKI, 2016), existem quatro tipos de classificações e, segundo eles, o principal bem jurídico a ser tutelado é a inviolabilidade da informação automatizada (dados). São eles: crimes informáticos impróprios, onde o computador é meio para executar o crime mas não existe a inviolabilidade da informação automatizada (ameaça, incitação ao crime); crimes informático próprios, em que o bem jurídico protegido é a inviolabilidade de dados(invasão de dispositivo informático); crimes mistos, onde a legislação penal se encarrega de proteger a inviolabilidade de dados e bem jurídico de natureza diversa (crime eleitoral) e o crime informático mediato ou direto que é aquele considerado o delito fim não informático que herdou a característica do meio para consumar o crime.

Por fim, há autores como Ferreira (2001 apud TATEOKI, 2016) e Crespo (2011 apud TATEOKI, 2016) que defendem somente duas modalidades: crimes informáticos próprios, praticados por meio da informática e sem ela o delito não ocorrerá (crime de inserção de dados falso em sistema de informações, artigo 313-A do CP) e os crimes informáticos impróprios, que podem ser praticados de várias formas, sendo elas por meio da informática ou não (crimes contra a honra, violação dos direitos do autor, estelionato, pornografia infantil).

3 SUJEITOS DOS CRIMES DE INFORMÁTICA E OS CRIMES DE INFORMÁTICA EM ESPÉCIE

3.1 Sujeitos dos Crimes de Informática

3.1.1 Sujeito ativo

3.1.1.1 Hacker (*White Hat*)

Comumente, para designarmos um criminoso de Internet, nos referimos ao termo *Hacker*. Porém, este não é o termo mais adequado. Os doutrinadores e os profissionais da informática preferem chamar os criminosos de *crackers*.

Os *Hackers* detêm um vasto conhecimento de informática, assim como os crackers, e sabem encontrar com facilidade qualquer brecha de segurança nos sistemas, porém, não alteram nem danificam nada. Os hackers muitas vezes são contratados por empresas que pretendem testar os seus sistemas de segurança, de modo a procurar por eventuais falhas que comprometam seus dados sigilosos ou o próprio funcionamento da empresa.

Nogueira (2008, p.61) discorre sobre o tema:

> HACKER – Este indivíduo em geral domina a informática e é muito inteligente, adora invadir sites, mas na maioria das vezes não com a finalidade de cometer crimes, costumam se desafiar entre si, para ver que consegue invadir tal sistema ou página na internet, isto apenas para mostrar como estamos vulneráveis no mundo virtual. Várias empresas estão contratando há tempos os Hackers para proteção de seus sistemas, banco de dados, seus segredos profissionais, fraudes eletrônicas, etc.

Outro termo associado aos *Hackers* é o “White Hat”. Este termo é utilizado para àqueles que conhecem brechas e falhas dos sistemas, mas, em tese, não cometem nenhum crime. Para Assunção (2008, p.13):

> Hacker White-Hat: Seria o “hacker do bem”, chamado de “hacker chapéu branco”. É aquela pessoa que se destaca nas empresas e instituições por ter um conhecimento mais elevado que seus colegas, devido ao autodidatismo e à paixão pelo que faz. Não chega a invadir sistemas e causar estragos, exceto ao realizar testes de intrusão. Resumindo: tem um vasto conhecimento, mas não o usa de forma banal e irresponsável.

Assim depreende-se dizer que os “White Hats” não procuram causar danos, mas isso não quer dizer que eles venham a cometer crimes. O fato de invadir um sistema sem autorização, por exemplo, ainda que sem alterar ou danificar nada, pode caracterizar um crime.

3.1.1.2 *Cracker*

Os *crackers* são os criminosos que possuem vasto conhecimento de informática e utilizam deste conhecimento para achar brechas nas redes virtuais de modo a causar danos a terceiros ou obter alguma informação confidencial.

Ao contrário dos *hackers* que são denominados de “White Hats”, os *crackers* recebem a denominação de “Black Hats”. Aponta Assunção (2008, p.13):

> Hacker Black-Hat: “Hacker do Mal” ou “chapéu negro”. Esse, sim, usa seus conhecimentos para roubar senhas, documentos, causar danos ou mesmo realizar espionagem industrial. Geralmente tem seus alvos bem definidos e podem passar semanas antes de conseguir acesso onde deseja, se o sistema for bem protegido.

É comum a confusão entre estes dois termos, sendo associado sempre ao criminoso virtual a expressão *hacker*, expressão esta que inicialmente designava uma pessoa com grande habilidade ou apreço por computação, conforme aponta Rufino (2002, p.16):

> Desde que apareceu nos meios de comunicação, o termo hacker perdeu a conotação romântica de outros tempos, pois se antes significava aficionado por computadores (a origem é ainda anterior) agora indica piratas eletrônicos ligados a crimes utilizando computadores. Bem que se tentou (e alguns ainda tentam) associar a esses últimos o termo cracker: “aqueles que quebram sistemas”, mas acredito que seja uma causa perdida.

> Visto que o termo ganhou uma carga pejorativa, os vendedores de serviço de segurança criaram a figura do “hacker ético”, para tentar minimizar o impacto que o termo hacker causa ao cliente, e é justamente a palavra “ética” que acaba fazendo toda a diferença.

Os *crackers* ainda são subdivididos conforme sua área de atuação ou nível de conhecimento: *phreaker*, *spammers*, *defacer* ou pichador virtual, *lammer* e *carders*.

Os *phreakers* são os *hackers* encarregados de burlar os sistemas das operadoras de telefonia. Eles clonam celulares, fazem escutas telefônicas sem autorização, alteram os sistemas de cobranças de telefones, etc. Segundo Rosa (2006, p.62), *phreaker* é:

> Especializado em telefonia, atua na obtenção de ligações telefônicas gratuitas e instalação de escutas, facilitando o ataque a sistemas a partir de acesso exterior, tornando-se invisíveis ao rastreamento ou colocando a responsabilidade em terceiros.

Defacer é todo aquele que coloca indevidamente textos ou figuras em sites de terceiros sem autorização, ou seja, ele faz uma “pichação virtual”. O autor do fato só poderá ser incriminado caso provoque ao dono do *site* algum prejuízo de cunho patrimonial. Somente o fato de colocar um texto ou figura não configura crime, visto que não acarreta por si só prejuízo patrimonial, e no Brasil essa conduta ainda não está tipificada.

Rufino (2002) afirma que os *hackers* são subdivididos por “facções” e afirma que existem, além de *Phraker* e *craking*, os *Virii, Warez, Carding e Coders*. Os *Virii* são os programadores e colecionadores de vírus de computador; os *Warez* estão encarregados da pirataria de *software*; os *Carding* manipulam cartões magnéticos e telefônicos e os *Coders* são os codificadores, conhecedores de programação e que se encarregam de explorar vulnerabilidades de programas.

São vastas as modalidades de *crackers*, não impedindo que um mesmo *hacker* possa ter conhecimento em duas ou mais áreas, como por exemplo, um indivíduo ter habilidade em *Phreaker* e *Coder*.

3.1.1.3. Outros sujeitos

Vale ressaltar que nem todo usuário da rede de computadores possui vastos conhecimentos de computação. Basta que saiba como usar um computador e

acessar a Internet, ou seja, são pessoas comuns. Podem-se citar como exemplos os crimes contra a honra (calúnia, difamação e injúria); pedofilia (no que se refere a adquirir, repassar conteúdo pornográfico envolvendo crianças e adolescentes).

3.1.2. Sujeito passivo

Podem ser sujeitos passivos nos crimes de informática toda e qualquer pessoa que utiliza um computador ou qualquer tecnologia informática (celular, *tablet* caixa eletrônico etc.), esteja ela conectada à Internet ou não. Para Nogueira (2008, p.63) “qualquer um de nós pode ser vítima, todos nós que temos acesso à rede mundial de computadores estamos arriscados a sermos vítimas dos delitos informáticos”.

3.2 Crimes em espécie

3.2.1 Crimes contra a Honra

Os crimes contra a honra estão previstos nos artigos 138 ao 145 do Código Penal, sendo que são três as espécies: Calúnia (art.138 do CP); Difamação (art.139 do CP) e Injúria (art. 140 do CP).

Comenta Mirabete (2003) que o crime de Calúnia é praticado por quem imputa, atribui a alguém a prática de crime, ou seja, é afirmar falsamente que o sujeito passivo praticou determinado delito. Para que haja a configuração de Calúnia, é necessário que a imputação verse sobre fato determinado, concreto, específico, embora não se exija que o sujeito ativo descreva suas circunstâncias, suas minúcias, seus pormenores. Pode ser cometido de maneira livre, por meio da palavra escrita ou oral, por gestos e até meios simbólicos. A imputação de contravenção não configura Calúnia, mas pode caracterizar Difamação.

Sobre Difamação, explica Teles (2004, p.271):

> A difamação é a imputação de um fato certo, determinado, capaz de macular a honra objetiva da pessoa. Não pode ser um fato típico de crime, pois aí haverá calúnia, mas, imputada a prática de um outro ilícito, uma contravenção penal ou um ilícito civil, poderá constituir difamação desde que tal fato seja ofensivo.
>
> Não é necessário que o fato seja ilícito, todavia deve ser daqueles que martirizam a reputação da vítima. Dizer que determinada pessoa dá-se a práticas homossexuais com seu motorista é, evidentemente, um fato ilícito mas que ofende a honra até do homossexual que mantém, perante o seu meio social, uma imagem de heterossexual.

Finalmente resta o crime de Injúria, que seguindo Mirabete (2003) a conduta típica é ofender a honra subjetiva do sujeito passivo, atingindo seus atributos morais (dignidade) ou físicos, intelectuais, sociais (decoro). Não há na injúria imputação de fatos precisos e determinados, como na calúnia ou difamação, mas apenas de fatos genéricos desonrosos ou de qualidades negativas da vítima.

Tais crimes contra a honra são praticados, na maioria das vezes, de forma oral, embora admitida a forma escrita, que não é muito comum. Estes delitos têm uma repercussão cada vez maior no mundo virtual, onde ocorrem de forma escrita ou gráfica, e podem ser vistos por qualquer pessoa que tenha acesso à rede. Entretanto, o anonimato dificulta a identificação do criminoso e há dificuldades na retirada do conteúdo ofensivo.

Estes crimes são bastante comuns na Internet pois, por estarem protegidas "atrás" de um computador, as pessoas se sentem motivadas a realizar estes delitos visto que o anonimato garante a segurança e o conforto delas. Os usuários utilizam de ferramentas como as redes sociais, *chats*, *blogs* etc., para ofender a honra de seus desafetos, seja imputando a estes falsamente um crime, um fato ofensivo a reputação ou mesmo ofendendo a dignidade e o decoro.

Para Castro (2003, p.16):

> Tanto a calúnia como a difamação protegem a honra objetiva e para a sua consumação é necessário que terceira pessoa tome conhecimento do fato. Se só o ofendido souber das agressões, não se consumará o crime. Diante disso, podemos afirmar que estes crimes podem ser praticados através de uma homepage ou em salas de bate-papo, nas conhecidas conversas on line. As ofensas proferidas em conversas on line podem ser conhecidas dos integrantes do canal ou das salas, ou dirigidas particularmente ao ofendido. Quando a ofensa puder ser conhecida por outrem além do próprio ofendido, resta consumada a infração. Todavia, quando a ofensa é dirigida só para o ofendido e ninguém toma conhecimento do seu conteúdo, não há crime de calunia e difamação. O mesmo raciocínio pode ser utilizado para as ofensas enviadas por e-mails. Se só a vítima utiliza, difícil é a configuração do crime.

> Todavia, se o e-mail é conjunto e o agente sabia desta condição, é possível a consumação. [...]
>
> O crime de injúria tutela honra subjetiva, sendo suficiente para sua configuração que o ofendido tome conhecimento do fato. Assim, este delito pode ser praticado por e-mail, nas salas de conversa, nas homepages, nos sites, etc.

Ao adentrar no assunto das redes sociais, Basso e Polido (2008, p.462) citam a violação do direito à honra e observam que há uma dificuldade do judiciário para entender como se dão as violações à honra no ambiente virtual:

> Em geral, os litígios relacionados aos direitos da personalidade na internet referem-se à violação dos direitos ao nome, à imagem, à honra e privacidade dos usuários. Nesses casos, o jurista encontra dificuldade em entender as armadilhas relacionadas ao armazenamento e circulação de informações no ambiente digital. O caso das redes de relacionamento social aponta para as hipóteses de apropriação injustificada de dados armazenados nos perfis de usuários, as quais servem de ponto de partida para a prática de ilícitos de violação de direitos da personalidade (e.g. sites ofensivos, intercâmbio e disseminação de mensagens difamatórias, utilização de fotos para endossar correspondência e interação com usuários de internet sem qualquer correspondência efetiva com o titular dos direitos de imagem associados, criação de perfis utilizando nome da pessoa sem autorização etc..) [...].

Portanto, a Internet permitiu um grande aumento nos casos relacionados aos crimes contra à honra uma vez que o número de dados e informações que circulam nas redes é enorme e isso dificulta o seu controle. Uma das causas do aumento de casos relacionados a este tipo de delito é o anonimato que a Internet proporciona aos seus usuários.

3.2.2 Racismo e Injúria Qualificada pelo Uso de Elemento Racial

Racismo, no conceito de Bulos (2003, p.255) é:

> Todo e qualquer tratamento discriminador da condição humana em que o agente dilacera a autoestima e o patrimônio moral de uma pessoa ou de um grupo de pessoas, tomando por critérios raça ou cor da pele, sexo, condição econômica, origem etc.

A Constituição da República Federativa do Brasil traz alguns dispositivos para coibir a prática do racismo. Dispõe os artigos 3º, IV; 4º, VIII; e 5º, XLII da CRFB:

> Art. 3º Constituem objetivos fundamentais da República Federativa do Brasil:

> IV – promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação.
>
> Art. 4º A República Federativa do Brasil rege-se nas suas relações internacionais pelos seguintes princípios:
>
> VIII – repúdio ao terrorismo e ao racismo;
>
> Art. 5º.
>
> XLII – a prática do racismo constitui crime inafiançável e imprescritível, sujeito à pena de reclusão, nos termos da lei.

Já Moraes (2007, p.230), para dar maior eficácia ao dispositivo constitucional, observa que o Código Penal prevê a injúria qualificada pelo uso de elemento racial:

> Acrescente-se, por fim, que o legislador ordinário, para garantir maior eficácia do preceito constitucional, protetor de igualdade e inimigo das discriminações, estabeleceu como figura típica diferenciada a injúria consistente na utilização de elementos referentes a raça, cor, etnia, religião ou origem, apenando-a com reclusão de um a três anos e multa (CP, art. 140, §3º).

A injúria qualificada pelo uso de elemento racial se caracteriza como um crime em que se ofende a honra, com palavras, termos ou gestos referentes à raça da vítima. Já no racismo, o agente deve praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, religião ou procedência nacional e assim impedir que a vítima exerça algum direito em razão das razões já mencionadas, conforme a Lei 7.716/89.

Deve-se frisar a modificação do artigo 140, §3º do Código Penal, pela Lei nº 12.033, de 29 de setembro de 2009 tornando ação penal pública condicionada à representação do ofendido os crimes de injúria em razão de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência.

Também é possível a ocorrência de preconceito racial no campo virtual que se dá de modo similar aos crimes contra a honra, em que são publicados textos, imagens ou vídeos de conteúdo ofensivo na Internet. Neste caso o crime está previsto no artigo 20 da Lei nº 7.716:

> Art. 20 Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional.
>
> Pena: reclusão de um a três anos e multa.

Nogueira (2008) cita o primeiro processo aberto no Brasil decorrente da prática de racismo na Internet, em janeiro de 2006. Os dois acusados eram estudantes e utilizaram uma rede social que atualmente não existe mais, o ORKUT, para a prática do delito.

Mesmo com a repressão legal, o racismo e a injúria qualificada pelo uso de elemento racial continuam a ocorrer e são uma prática muito comum nas redes sociais. Inúmeros são os casos de repercussão nacional em que atores e atrizes de telenovelas, repórteres negros ou negras e pessoas comuns são vítimas daquelas que se escondem por uma tela de computador e praticam estes delitos.

3.2.3 Pedofilia

Pedofilia, na concepção de Nogueira (2008, p.97), não é propriamente um crime, mas um desvio sexual. Entretanto, passa a ser punido quem, em razão de sua atração sexual, pratica alguma conduta sexual que envolva criança ou adolescente, proibidas por lei.

> Uma parafilia na qual a atração sexual de um indivíduo adulto está dirigida primariamente para crianças pré-púberes ou ao redor da puberdade. [...]. A pedofilia por si só, não é um crime, mas sim, um estado psicológico, e um desvio sexual. A pessoa pedófila passa a cometer um crime quando, baseado em seus desejos sexuais, comete atos criminosos como abusar sexualmente de crianças ou divulgar ou produzir pornografia infantil.

No Brasil há leis que protegem a criança e o adolescente da prática de indivíduos que possuam este desvio sexual, como o próprio Código Penal e a Lei nº 8.069, de 13 de julho de 1990. O ECA, ou Estatuto da Criança e do Adolescente, que é a lei 8.069/1990, pune mais severamente a divulgação de material pornográfico das vítimas.

A pedofilia, como crime de informática, acontece quando os agentes trocam entre si materiais pornográficos, sejam fotos ou vídeos, envolvendo crianças e adolescentes. Não é um crime que envolva muito conhecimento por parte do criminoso, visto que só é necessário que ele saiba usar algumas ferramentas como *e-mail*, programas ou aplicativos que enviem mensagens, redes sociais etc., para cometer o ilícito penal.

O Estatuto da Criança e do Adolescente também procura combater ao máximo a pedofilia. No ano de 2008 foram promovidas algumas alterações para que fossem punidos aqueles que mandassem *e-mails* que contivessem fotos ou qualquer outro tipo de material que envolvesse sexo entre crianças e/ou adolescentes, já que antes não havia a previsão deste tipo de prática pela Lei.

3.2.4 Estelionato

O crime de estelionato se encontra tipificado no artigo 171, caput, do Código Penal e ele descreve: “Obter, para si ou para outrem, vantagem ilícita em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento”.

Para Greco (2010, p.485) o crime de estelionato é constituído “pelo binômio vantagem ilícita / prejuízo alheio. A conduta do agente, portanto, deve ser dirigida a obter vantagem ilícita em prejuízo alheio. ”

O crime de estelionato exige quatro requisitos, obrigatórios para sua caracterização: obtenção de vantagem ilícita; causar prejuízo a outra pessoa; uso de meio de ardil, ou artimanha e enganar alguém ou a leva-lo a erro. A ausência de um dos quatro elementos, seja qual for, impede a caracterização do estelionato. O crime aceita apenas a forma dolosa, ou seja, que haja real intenção de lesar, não havendo previsão forma culposa, ou sem intenção.

O delito de estelionato realizado na Internet também é conhecido por estelionato eletrônico e pode ser realizado tanto por pessoa que tenha grandes conhecimentos em informática como pessoa que tenha pouco conhecimento, sendo apenas um simples usuário da Internet.

O agente deste tipo de crime utiliza meios ardilosos e sofisticados para enganar as vítimas, penetrando em redes locais, e criando artifícios que, de alguma forma, possam garantir a percepção de dinheiro de maneira ilícita. BIASOLI (2010) explica de forma sucinta como ocorreria a prática do delito de estelionato na Internet:

> Como exemplo de estelionato praticado na Internet por um usuário Cracker, temos, a obtenção de dinheiro da vítima, por meio de transferência bancária para uma conta de posse do Cracker, ou de outrem. Isto ocorre mediante a criação de sites similares aos utilizados por bancos, sendo armazenados na Internet, e concomitantemente o Cracker desenvolve mensagens atrativas como fosse de autoria do banco da vítima, que é encaminhada à vítima por

> meio do correio eletrônico, e ao ser acessada, automaticamente será direcionada ao site similar de seu banco, ou seja, aquele criado pelo Cracker, possibilitando que, ao ser feito pela vítima qualquer transferência bancária, na verdade o dinheiro será transferido para uma outra conta que o Cracker previamente tenha registrado.

No que tange ao estelionato praticado através de sistemas informáticos, entende Ferreira (2005, p.250):

> A figura do estelionato, prevista no art. 171 do Código Penal brasileiro de 1940, que consiste no emprego de meios fraudulentos para a obtenção de ilícita vantagem, abrange os exemplos mais conhecidos e mais frequentes dessas atuações criminosas, tanto no Brasil quanto nos demais países. Compreende tanto o caso das transferências fraudulentas de fundos nas contas bancárias quantos os casos de frações de quantias, ou contas "arredondadas", nos cálculos de clientes ou da empresa, acumulando-se o dinheiro lentamente na conta pessoal do agente. Ou ainda o uso de cartão personalizado, fornecido pelos bancos para permitir o acesso às contas eletrônicas através de um código pessoal, abusivamente utilizado por alguém que o tenha furtado, encontrado ou falsificado.

Porém deve-se analisar caso a caso para que se estabeleça que o crime a ser praticado é o de estelionato. No caso das transações bancárias fraudulentas, trazidos pelo exemplo de Ferreira, no chamado *Internet Banking*, não se pode aplicar o artigo 171 do Código Penal, mas sim o crime de furto previsto no artigo 155 do código repressivo.

O STF já decidiu sobre o tema, no Conflito de Competência nº 72.738-RS, que no caso das fraudes em relações bancárias se aplica o Art. 155, §4º, II do Código Penal, ou seja, furto qualificado. Isto porque no caso do estelionato tem-se como característica a entrega do bem de forma espontânea através de fraude, já no furto não há concordância por parte do sujeito passivo, conforme bem explica a Ministra Relatora Thereza de Assis Moura em seu voto:

> O furto mediante fraude, escalada ou destreza não se confunde com o estelionato. No primeiro, a fraude visa a diminuir a vigilância da vítima, sem que esta perceba que está desapossada; há a discordância expressa ou presumida do titular do direito patrimonial em relação à conduta do agente. No segundo, a fraude visa a fazer com que a vítima incida em erro e, espontaneamente, entregue o bem ao agente; o consentimento da vítima integra a própria figura delituosa.

Tal entendimento não significa que não possa ser cometido o crime de estelionato. Castro (2003, p.31) fala ainda de algumas possibilidades da prática deste crime na informática:

> O crime de estelionato pressupõe dois resultados: vantagem ilícita e prejuízo alheio. Este resultado deve ser obtido mediante artifício, ardil ou qualquer outro meio fraudulento. É exatamente aqui que entra a informática. O agente pode utilizar homepages, sites, conversas online e e-mails para induzir o lesado a erro, seja mediante ardil, artifício ou qualquer meio.

Nogueira (2008, p.180) ainda cita alguns exemplos em que se procura enganar os usuários da rede de computadores:

> Muitas pessoas receberam e-mail pedindo para se recadastrarem na Receita Federal, pois seu CPF iria ser cancelado. Outro e-mail muito conhecido, foi sobre o recadastramento no Tribunal Superior Eleitoral, avisando a pessoa da necessidade imediata de enviar seus dados completos, pois eu título de eleitor seria cancelado. Este tipo de e-mail é enviado aos milhões e as pessoas com medo acabam respondendo, e seus dados vão parar nas mãos de crackers e serão usados para fins ilícitos, como na compra de alguma mercadoria, financiamentos e falsificação de algum documento para cometerem alguns crimes.

A seguir, tem-se um julgamento de Apelação nº 1023474-16.2014.8.26.0576 pelo TJ de São Paulo, em um caso de compra e venda de veículo por anúncio veiculado na Internet:

> AÇÃO DE RESSARCIMENTO C.C. INDENIZAÇÃO POR DANOS MORAIS. COMPRA E VENDA DE VEÍCULO. FRAUDE PRATICADA POR TERCEIRO POR MEIO DE ANÚNCIO VEICULADO PELA INTERNET. ESTELIONATO CONFIGURADO. CULPA CONCORRENTE DAS PARTES.
> Prática de estelionato por terceiro que se utilizou da internet para fraudar pessoa interessada na aquisição de veículo que se consumou em razão da condução do negócio jurídico de forma negligente pela concessionária. Por outro lado, o comportamento imprudente da consumidora que mesmo desconfiada do preço anunciado abaixo do mercado não verificou a regularidade dos termos do negócio ofertado contribuiu para a ocorrência do dano. Concorrência de culpas que enseja a responsabilidade de ambas as partes, de modo que cada uma delas deve arcar com metade do prejuízo financeiro reclamado nos autos. Recurso parcialmente provido.

3.2.5 Pichação Virtual

Também denominada de *defacement*, a pichação virtual se dá quando um *cracker* consegue invadir qualquer *site* fazendo alterações em sua estrutura, como deixando seu nome ou assinatura no *layout* da página virtual ou inserindo figuras nela sem a autorização do administrador de um site.

Nogueira (2008, p.62) trata dos objetivos principais dos pichadores virtuais:

> Estes adoram violar algum site, a maioria do poder público, como do FBI, Pentágono, Supremo Tribunal Federal, INSS e lá deixar sua marca, as vezes acontece algum tipo de protesto político ou religioso com esse tipo de invasão, ou podermos chamar de 'manifesto', normalmente não causam danos.

Antes do advento da Lei nº 12.737/12, a pichação virtual era um crime sem tipificação e só era aberto um processo criminal quando o *cracker* provocava ao proprietário do *site* algum tipo de dano, previsto no artigo 163 do Código Penal, e este devia ter valor patrimonial. Após a Lei, passou a ser abrangido pelo artigo 154-A do CP e caso haja prejuízo econômico, aumenta-se a pena de um sexto a um terço:

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

3.2.6 Dano

O crime de dano está previsto no artigo 163 do Código Penal e dispõe:

> Art. 163 – Destruir, inutilizar ou deteriorar coisa alheia:
>
> Pena – detenção, de um a seis meses e multa
>
> Dano qualificado
>
> Parágrafo Único – se o crime é cometido:
>
> I – com violência à pessoa ou grave ameaça;
>
> II – com emprego de substância inflamável ou explosiva, se o fato não constitui crime mais grave
>
> III – contra o patrimônio da União, Estado, Município, empresa concessionária de serviços públicos ou sociedade de economia mista;
>
> IV – por motivo egoístico ou com prejuízo considerável para a vítima:

> Pena – detenção, de seis meses a três anos, e multa, além da pena correspondente à violência.

Antes do advento da Lei 12.737/12, haviam divergências doutrinárias sob a aplicação do crime de dano para os casos de destruição ou inutilização de arquivos digitais de terceiros. Para alguns doutrinadores era perfeitamente possível a aplicação do artigo 163 do CP, ainda que o arquivo não tivesse valor patrimonial, não sendo necessário a criação de um novo tipo penal para o dano ocasionado através da informática (VIANA, 2003).

Para Castro (2003), não poderia ser aplicado o artigo 163 do Código Penal para a destruição, inutilização ou deterioração de arquivos digitais porque só poderia ser utilizado o artigo citado caso o arquivo tivesse algum valor material.

Já Ferreira (2005, p.261) entendia que:

> Certas condutas ofensivas aos sistemas informáticos ou telemáticos ou ao uso do computador, na verdade não se adaptam às figuras penais existentes na nossa legislação, seja as que constituem crimes informáticos propriamente ditos, seja as que constituem como crimes de legislação comum ou especial praticados por intermédio da informática ou dos computadores. Isso vale também para o delito de dano, que nessa matéria ultrapassa em muito os limites próprios do art. 163 do Código Penal, [...].
> Parece então ser apropriada a criação de um novo tipo penal, o do dano informático, consistente na destruição, alteração ou supressão de dados informáticos com o fim de produzir prejuízo ao usuário ou a terceiros, o que viria resolver inúmeros problemas existentes, atualmente sem uma resposta penal.

Enfim a Lei 12.737 de novembro de 2012 passou a tutelar as condutas previstas no caput do crime de dano dos dados informáticos adicionando o artigo 154-A ao Código Penal. Nele está previsto:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

Assim, qualquer ato que vise alterar ou destruir dados virtuais, independente se causem prejuízo econômico ou não, estão sujeitos a punição pelo artigo supramencionado.

3.2.7 Disseminação de Vírus, *Worms* e similares

Vírus, segundo Tamega (2003, p.40), são:

> Programas desenvolvidos para alterar nociva e clandestinamente softwares instalados em um computador, têm comportamento semelhante ao vírus biológico: multiplicam-se, precisam de um hospedeiro, esperam o momento certo para o ataque e tentam se esconder para não serem exterminados.

Já Rosa (2005, p.69) entende que "Vírus é o segmento de programa de computador capaz de mudar a estrutura do software do sistema e destruir ou alterar dados ou programas ou outras ações nocivas, com ou sem o conhecimento do autor".

Os *worms* são espécies de vírus que se auto reproduzem sem alterar o conteúdo do arquivo infectado e são imperceptíveis ao usuário do sistema e trocam constantemente de nome (NETO, 2011).

A disseminação e a contaminação dos vírus em computadores antes não eram consideradas crimes pelo ordenamento jurídico brasileiro. Só poderia ser punido aquele que ocasionasse dano patrimonial a terceiro e era aplicado a este o crime do artigo 163 do Código Penal. Com a Lei 12.737 de 2012, em seu artigo 154-A, passou a abarcar a prática de disseminar estes programas nocivos, tornando a disseminação e contaminação dos vírus como fatos típicos no código repressivo.

3.2.8 Violação dos Direitos do Autor

As violações dos direitos do autor são associadas ao termo pirataria virtual, como observa Galdemann (2001, p.86):

> Chama-se vulgarmente de pirataria à atividade de copiar ou reproduzir, bem como utilizar indevidamente– isto é, sem a expressa autorização dos respectivos titulares – livros ou outros impressos em geral, gravações de sons e/ ou imagens, software de computadores, ou, ainda, qualquer outro suporte físico que contenha obras intelectuais legalmente protegidas.

É um crime que, para alguns, deve ser severamente punido. Para outros, só configura crime quando há intenção lucrativa no compartilhamento de arquivos.

Mesmo que se confirme que a pirataria virtual é um crime e, como tal, deve punir aqueles que infringirem a lei, é uma conduta de difícil controle, visto que

milhares de usuários da Internet faz *downloads* ilegais de obras, músicas, filmes, livros etc..

Os Estados Unidos dificultaram bastante a prática deste tipo de crime ao impor leis mais severas para combater firmemente os infratores de direitos autorais. Ante a pressão de muitas gravadoras de músicas, o país processou e condenou várias pessoas para que amedrontasse as demais e parassem de desobedecer aos direitos autorais.

No Brasil, o crime de violação de direitos autorais está previsto no artigo 184 do Código Penal:

> Art. 184. Violar direitos de autor e os que lhe são conexos:
>
> Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa
>
> §1º Se a violação constituir em reprodução total ou parcial, com intuito de lucro direto ou indireto, por qualquer meio ou processo, de obra intelectual, interpretação ou execução ou fonograma, sem autorização expressa do autor, do artista intérprete ou executante, do produtor, conforme o caso, ou de quem os represente:
>
> Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
>
> §2º Na mesma pena do §1º incorre quem, com o intuito de lucro direto ou indireto, distribui, vende, expõe à venda, aluga, introduz no País, adquire, oculta, tem em depósito, original ou cópia de obra intelectual ou fonograma reproduzido com violação do direito de autor, do direito de artista intérprete ou executante ou do direito do produtor de fonograma, ou, ainda, aluga original ou cópia de obra intelectual ou fonograma, sem a expressa autorização dos titulares dos direitos ou de quem os represente.
>
> §3º Se a violação consistir no oferecimento ao público, mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção da obra ou produção para recebê-la em um tempo e lugar previamente determinados por quem formula a demanda, com intuito de lucro, direto ou indireto, sem autorização expressa, conforme o caso, do autor, do artista intérprete ou executante, do produtor de fonograma, ou de quem os represente:
>
> Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
>
> §4º O disposto nos §§1º, 2º e 3º não se aplica quando se tratar de exceção ou limitação ao direito de autor ou os que lhe são conexos, em conformidade com o previsto na Lei n. 9.610, de 19 de fevereiro de 1998, nem a cópia de obra intelectual ou fonograma, em um só exemplar, para uso privado do copista, sem intuito de lucro direto ou indireto.

Sobre o que diz o caput do artigo 184, doutrina Prado (2008, p.133-134):

> A conduta insculpida no artigo 184, caput consiste em violar (infringir, ofender, transgredir) direitos de autor (interesses patrimoniais e morais) e os

> que lhe são conexos (direitos correlatos aos de autor – dos artistas intérpretes ou executantes – arts. 90 a 92, produtores fonográficos – arts. 93 e 94 – e das empresas de radiodifusão – art. 95 -, constantes da Lei 9.610/1998). Trata-se de norma penal em branco que precisa ser complementada por outra norma; no caso em apreço, pela Lei 9.610/1998.

Porém, no Brasil, referentes aos problemas com a pirataria virtual, o país não age de forma eficaz para combatê-la. Em geral a repressão está voltada para aqueles que colocam ou facilitam o compartilhamento de arquivos que transgridam os direitos autorais, e não para aqueles que adquiram esses arquivos. No julgamento de Agravo de Instrumento nº 561.551-4, o Tribunal de Justiça do Paraná impediu que a empresa Cadari Tecnologia da Informação Ltda. disponibilizasse o programa “K-Lite Nitro”, programa este que possibilitava o compartilhamento de arquivos digitais entre os internautas:

> AGRAVO DE INSTRUMENTO. TUTELA INIBITÓRIA. PRETENDIDA ANTECIPAÇÃO LIMINAR DOS SEUS EFEITOS. Disponibilização pública de "software", denominado "k-lite nitro", para conexão às redes "peer-to-peer" (p2p) possibilitando o "download" de músicas pela "internet". Plausibilidade da ocorrência de conduta antijurídica (civil e criminal). Risco na demora presente pretensão no sentido de ser removido o ilícito mediante ordem que impeça a continuação dessa atividade. Decisão do juiz da causa apenas determinando a inserção de "banners" nos "sites" comunicando aos internautas a natureza ilícita dessa operação sem o pagamento de direitos autorais. Medida que não se mostra apta a tornar efetiva a tutela jurisdicional almejada. Recurso provido parcialmente para determinar a instalação, em princípio, como providência visando a obtenção do resultado prático equivalente ao do adimplemento, de dispositivo (filtro) no referido programa de computador, sob pena de multa diária, para impedir o compartilhamento de arquivos e/ou fonogramas musicais protegidos pela lei federal nº 9.610/1998. Remessa, outrossim, de peças dos autos ao excelentíssimo senhor procurador geral de justiça.

O próprio Código penal prevê, em seu artigo 184 §4º, a possibilidade de não se aplicar o crime. Prado (2008, p.136) traz a aplicabilidade do referido dispositivo:

> O art. 184, §4º restringe o âmbito de abrangência da tipicidade ao prescrever que não se aplicará o disposto nos parágrafos anteriores quando “se tratar de exceção ou limitação ao direito de autor ou os que lhe são conexos, em conformidade com o previsto na Lei 9.610, de 19 de fevereiro de 1998, nem a cópia da obra intelectual ou fonograma, em um só exemplar, para uso privado do copista, sem intuito de lucro direto ou indireto”. As exceções ou limitações apontadas no parágrafo em análise são as constantes dos artigos 46, 47 e 48 da Lei 9.610/1998, de modo que ocorrendo qualquer das hipóteses ali previstas não caracterizará ofensa aos direitos autorais e a conduta será atípica.

Importante ressaltar é o caso da violação dos direitos autorais da propriedade intelectual de *software*, protegido pela Lei 9.609 de 19 de fevereiro de 1998. Nogueira (2008, p.165) traz o conceito de pirataria de *software*:

> Ao contrário de outros itens que você adquire, os aplicativos de software e as fontes que você compra não lhe pertencem. Você se torna um usuário licenciado – você adquire o direito de usar o software em um único computador, mas não pode inserir cópias em outras máquinas nem passar o software adiante para colegas. A pirataria de software é a distribuição e/ou a reprodução ilegais de aplicativos de softwares ou fontes da Adobe para uso comercial ou pessoal. Seja a pirataria de software deliberada ou não, ela é ilegal e pode ser punida por lei.

Wachovicz (2004, p.339-340) entende que aos programas de computador (*software*) se aplica o Direito Autoral e não os Direitos Industriais:

> O programa de computador em si desprende-se de todo e qualquer meio físico hardware) que possa lhe servir de suporte. Dessa maneira, é possível classificá-lo enquanto linguagem de programação como um bem jurídico incorpóreo, também chamado de imaterial, pois não possui existência física, mas abstrata. E dessa forma o software é considerado pela doutrina dominante como afeto e tutelado pelo Direito Autoral, e não pelo Direito Industrial.
>
> O regime de proteção à propriedade intelectual de programa de computador é conferido às obras literárias pela legislação de direitos autorais.

Motta (2008, p.222) ainda traça as principais aplicações da Lei de Software:

> O regime de proteção à propriedade intelectual do software está determinado pelo artigo 2º da Lei do Software. É o mesmo conferido às obras literárias pela Lei da Propriedade Intelectual. Entretanto, exceto com relação ao direito do autor do software de reivindicar a autoria do programa de computador e o direito do autor de opor-se a alterações não autorizadas, nos termos da lei, não se aplicam aos softwares as disposições relativas aos direitos morais, nos termos do §1º do artigo 2º da Lei do Software.
>
> Pelo §2º do artigo 2º também verificamos que ao autor do software é garantida a tutela dos direitos relativos ao software pelo prazo de 50 anos, contados a partir de 1º de janeiro do ano subsequente ao de sua publicação ou, na ausência desta, da sua criação. De acordo com o §3º do artigo 2º, da mesma forma que trata para qualquer propriedade intelectual, a proteção aos direitos de que trata a Lei do Software independe de registro.

A Lei 9.609/98 prevê a pena de detenção de seis meses a dois anos ou multa para quem violar este dispositivo. Caso da violação seja a reprodução, ainda que parcial do programa para atividades de comércio não autorizado, a pena é de reclusão de um a quatro anos e multa.

3.2.9 Cyberterrorismo

Antes de adentrarmos na discussão sobre o cyberterrorismo, deve-se saber primeiramente o que é terrorismo. Segundo Leite Filho (2004, p.46):

> Definir terrorismo não é uma tarefa fácil porque, em vista da relatividade do termo e da possibilidade de este assumir diversas acepções, é difícil alcançar um conceito universal que explique sua verdadeira natureza. Jimenez de Asúa define terrorismo como sendo um crime ou uma série de crimes que se tipificam pelo alarme que produzem, ordinariamente motivado pelos meios de estrado que o terrorista costuma usar. Neste ponto reside um dos principais problemas que encontramos ao tentar definir a prática do terrorismo. Para uma parte da doutrina, o terrorismo é um crime comum como outro qualquer, enquanto para outra, trata-se de crime eminentemente político.

Seguindo o raciocínio deste mesmo autor, cyberterrorismo é um ataque premeditado, com motivação política contra o sistema de informações de um computador, programas de computador ou arquivos armazenados em sistemas de inteligência artificial. Resulta em danos consideráveis a pessoa ou coisas e surge do descontentamento de certos grupos com o sistema político vigente na sociedade para causar uma espécie de pânico generalizado (LEITE FILHO, 2004).

Os *crackers* que praticam este crime objetivam a confusão ou danos aos sistemas informáticos, principalmente de órgãos governamentais, para causar pânico através dos meios tecnológicos.

Nogueira (2008) trata de algumas condutas praticadas pelos terroristas na Internet, entre elas estão:

a) Planejamento de ataques em massa;
b) Divulgação de manuais de guerrilha;
c) Preparação de bombas;
d) Realização e organização de ataques em massa;
e) Envio de mensagens de ódio;
f) Propaganda com a divulgação de vídeos com mensagens terroristas;
g) Divulgação de boatos para aterrorizar algum país ou população especifica;
h) Como realizar ataques terroristas

Um dos países que teme um ataque cybeterrorista é os Estados Unidos, que por ter serviços como fornecimento de água, controle de vôos e eletricidade conectados à rede mundial, despende várias medidas para evitar as investidas virtuais dos terroristas.

Esta preocupação se intensificou ainda mais após os ataques de 11 de setembro, segundo Finkelstein (2008, p.431):

> Após os ataques terroristas de 11 de setembro de 2001, os estados Unidos passaram a se preocupar intensamente com a ocorrência de crimes informáticos, uma vez que foi amplamente noticiado pela imprensa que os terroristas utilizaram-se dos meios eletrônicos para se comunicar e arquitetar os ataques que chocaram o mundo.

Assim, fica evidente a preocupação de certos países com o cyberterrorismo. Este tipo de crime acarreta tantos problemas quanto um crime de terrorismo comum e de certa forma é muito mais fácil de ser praticado, pois pode ser realizado de qualquer lugar do mundo e o agente ou agentes têm a possibilidade de se livrarem das provas e podem resguardar seu anonimato, já que muitas vezes quem realiza este tipo de atividade é um profundo conhecedor de informática.

3.2.10 Interceptação Informática

A Constituição pátria protege a inviolabilidade da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, em seu art. 5º, XII:

> XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução penal;

A Lei nº 9.296/96, que regulamenta a parte final do inciso XII da Constituição Federal, fez uma extensão para a informática, em seu art. 1º, Parágrafo Único:

> Art. 1º. A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.
>
> Parágrafo Único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.

A Lei nº 9.296/96 ainda prevê, em seu artigo 10, a punição para quem interceptar comunicações de informática:

> Art. 10. Constitui crime realizar interceptações de comunicações telefônicas, de informática ou telemática, ou quebrar segredo de Justiça, sem autorização judicial ou com objetivos não autorizados em lei.
>
> Pena: reclusão, de dois a quatro anos, e multa.

Ferreira (2005, p.260) entende que esse artigo só pode ser usado para obtenção de provas para fins policiais ou judiciais:

> Nos termos em que foi estabelecido esse tipo penal, a conduta criminosa fica limitada aos fins visados pela lei em que se insere, ou seja, a obtenção de provas para fins policiais ou processuais, o que limita bastante a incriminação, pois se a interceptação informática não adequar-se ao modelo proposto o autor incidirá apenas no delito de violação de comunicação, previsto no art. 151, §1º do Código Penal, punido mais brandamente.

Dispõe o art. 151 do Código Penal:

> Art. 151. Devassar indevidamente o conteúdo de correspondência fechada dirigida a outrem:
>
> Pena – detenção, de 1 (um) a 6 (seis) meses, ou multa
>
> §1º Na mesma pena incorre:
>
> I – quem se apossa indevidamente de correspondência alheia, embora não fechada e, no todo ou em parte, a sonega ou destrói

Porém, Nucci (2007, p.649) afirma:

> Derrogação do art. 151: as figuras típicas previstas no caput e no §1º foram substituídas pela lei que rege os serviços postais – especial e mais nova -, o que se pode constatar pela leitura do art. 40: 'Devassar indevidamente o conteúdo de correspondência fechada dirigida a outrem: Pena – detenção, até seis meses, ou pagamento não excedente a vinte dias-multa. §1º Incorre nas mesmas penas que se apossa indevidamente de correspondência alheia, embora não fechada, para sonegá-la ou destruí-la, no todo ou em parte. §2º As penas aumentam-se da metade se há dano para outrem'.

Nucci (2007) entende que devassar é descobrir o conteúdo da correspondência sem necessariamente abri-la e no caso do §1º, apossar é tomar para si a correspondência de outra pessoa.

Portanto, há dois caminhos: será aplicada a Lei 9.296/96 no caso de interceptação informática sem autorização judicial, em que a pena será mais severa,

e para os demais casos, a aplicação da Lei 6.538/78 que trata dos crimes de violação de correspondência.

4 DA PROVA E A DIFICULDADE DE APURAÇÃO DOS FATOS QUE ENSEJAM OS DELITOS INFORMÁTICOS

A responsabilidade criminal só pode ser anunciada e a sanção penal cabível só pode ser aplicada quando houver certeza da prática do ilícito penal e de sua autoria. A prova tem a finalidade de fornecer ao juiz todos os elementos objetivos e subjetivos e os acontecimentos importantes para que ele possa solucionar os conflitos sobre o fato criminoso e sua autoria, assim aplicando a pena cabível ou medida de segurança.

Segundo Tourinho (2009, p.522):

> [...] Provar é, antes de mais nada, estabelecer a existência da verdade; e as provas são os meios pelos quais se procura estabelecê-la. É demonstrar a veracidade do que se afirma, do que se alega. Entendem-se, também, por prova, de ordinário, os elementos produzidos pelas partes ou pelo próprio Juiz visando a estabelecer, dentro do processo, a existência de certos fatos. É o instrumento de verificação do *thema probandum*.

Uma das grandes dificuldades relacionadas à investigação dos crimes informáticos é a escassez de provas que demonstrem a conduta delituosa.

“As infrações praticadas pelos criminosos no ambiente informático, muitas vezes, não deixam rastros, e devido a obscuridade da rede, o autor do crime fica à sombra do anonimato” (MATOS, 2014). As provas pertencentes à prática destes

delitos sofrem de uma fragilidade quanto a sua obtenção, seja pela autoridade policial quando prende o autor em flagrante ou pelo perito que busca encontrá-las.

Importante destacar o papel das provas ilícitas decorrentes das investigações realizadas sem autorização no ambiente virtual, violando o artigo 5º, inciso LVI, da Constituição e o artigo 157 do Código de Processo Penal. Como nas investigações com quebra de sigilo telefônico, também é necessária uma prévia autorização da autoridade judiciária para realizar a apuração do crime praticado na rede virtual.

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> LVI - são inadmissíveis, no processo, as provas obtidas por meios ilícitos;
>
> Art. 157. São inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais.

As provas obtidas por meios ilícitos não são aceitas no processo penal. A prova ilícita é aquela obtida por meios que não estão disciplinados no direito material. Não se deve confundir prova ilícita com prova ilegítima, já que esta é adquirida em desacordo com o direito processual.

> Saliente-se que a doutrina constitucional passou a atenuar a vedação das provas ilícitas, visando corrigir distorções a que a rigidez da exclusão poderia levar em casos de excepcional gravidade. Esta atenuação prevê, com base no Princípio da Proporcionalidade, hipóteses em que as provas ilícitas, em caráter excepcional e em casos extremamente graves, poderão ser utilizadas, pois nenhuma liberdade pública é absoluta, havendo possibilidade, em casos delicados, em que se percebe que o direito tutelado é mais importante que o direito à intimidade, segredo, liberdade de comunicação, por exemplo, de permitir-se sua utilização. (MORAES, 2010, p.112-113)

O INT (Instituto Nacional de Tecnologia) é o órgão responsável pela atribuição de autenticidade, integridade e validade jurídica aos documentos eletrônicos no Brasil. No entanto, nem toda prova obtida pelo meio eletrônico é admitida pelo Direito como um documento com validade jurídica, pois muitos doutrinadores acreditam não constituir uma prática que seja totalmente confiável.

Existe a discussão sobre o uso de documento eletrônico como prova no ordenamento jurídico brasileiro. Grande parte da doutrina entende que é admissível, porém se discute se o documento de origem eletrônica seria prova documental ou

pericial. A teoria mais adotada é aquela que conceitua como prova pericial, já que carecem de perícia técnica.

Sobre o determinado quesito, Barros (2011, p.126) afirma:

> Com efeito, se a infração penal for praticada por meio da Internet, é necessário identificar a máquina utilizada. 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.

Portanto, é duvidoso a atribuição de prova a determinado sujeito devido ao fato do computador, ou aparato tecnológico que está sendo utilizado para praticar delitos, resguardar o anonimato do indivíduo. Mesmo com a localização do endereço IP, deve-se proceder a uma perícia minuciosa para identificar o verdadeiro autor do ato já que o mesmo computador pode ser utilizado por mais de uma pessoa.

As provas obtidas possuem grande risco de perecimento e por isso devem ser coletadas com cuidado, rapidez e atenção para que não desapareçam e garantam a punição do agente infrator.

4.1 Da realização da perícia para a obtenção de provas

As provas dos crimes praticados pelo computador são coletadas por pessoas qualificadas ou peritos que tenham a competência técnica para a realização dos procedimentos técnicos para a obtenção de provas.

Primeiramente, para a coleta da prova, deve-se fazer uma perícia. Os crimes informáticos são caracterizados por requerer uma produção de prova pericial, pois precisam de um parecer de um profissional especializado em conhecimentos técnicos-científicos relacionados aos meios computacionais.

A perícia, como todo meio de produção de prova, é um instituto do direito processual e consiste numa manifestação técnico-científica que se materializa por meio de um laudo que servirá de base para a fundamentação de medida cautelar, bem como sentença judicial (KERR, 2011).

Conforme Aranha (1994, apud KERR, 2011), a perícia consiste em uma manifestação eminentemente técnica mediante a qual o experto nomeado emite uma declaração de ciência, uma afirmação de um juízo ou então, ambas simultaneamente. Sendo que, a função do perito pode restringir-se ao relato técnico das impressões colhidas, consistindo tão somente numa declaração de ciência. Ao passo que, em uma outra situação poderá ser requisitado a interpretar ou apreciar cientificamente um fato, emitindo um juízo. Por fim, poderá ser solicitado a realizar ambas as ações, ou seja, por primeiro, examinar tecnicamente o fato e, em seguida, emitir um juízo.

Sendo uma declaração de ciência ou emissão de juízo, a manifestação do perito, se acatada, serve de base para a fundamentação do juiz, podendo ser o único meio de prova disponível.

Relativamente aos crimes contra a propriedade imaterial tais como violação da propriedade de computador, que é um crime informático, e que pode deixar vestígios, a prova pericial é disciplinada por normas processuais específicas. O exame do corpo de delito constitui elemento essencial de procedibilidade para recebimento da queixa ou denúncia, como aduz o artigo 525 do Código de Processo Penal: “ No caso de haver o crime deixado vestígio, a queixa ou a denúncia não será recebida se não for instruída com o exame pericial dos objetos que constituam o corpo de delito. ”

O crime praticado pelo computador é passível de investigação assim como o crime praticado no meio físico, principalmente por deixar vestígios. Parte dos procedimentos relativos as investigações de ambos os delitos são semelhantes mesmo que as evidências dos crimes informáticos estejam em um grau de complexidade diferente. “ No que diz respeito ao procedimento relacionado à prova pericial em meios computacionais, podemos dividi-lo em três momentos, quais sejam: iniciativa, execução e materialização ou exteriorização” (KERR, 2011, p.55).

De acordo com Kerr (2011, p.55-56):

> A iniciativa do exame pericial dependerá diretamente do momento em que se encontra a investigação do fato delituoso. Se estiver na fase do inquérito policial, fase extrajudicial, portanto, a iniciativa é da autoridade policial. Caso já tenha sido proposta ação, ou seja, esteja já na fase judicial, o juiz poderá requerer a perícia de ofício e de imediato, quando obrigatória, ou mediante provocação, nos demais casos. Contudo, no caso de não ser obrigatória, se requerida pelas partes, poderá ser indeferida pela autoridade policial ou pelo juiz, caso não seja necessária, nos termos do artigo 184 do Código de

> Processo Penal, que preceitua: “Salvo o caso de exame de corpo de delito, o juiz ou a autoridade policial negará a perícia requerida pelas partes, quando não for necessária ao esclarecimento da verdade.

Quando a oportunidade, embora não haja a disciplina pelo Código de Processo Penal, a regra mais segura, considerando os vestígios deixados pelo crime, é que sejam obtidos rapidamente, implicando em providências ágeis a serem adotadas pela autoridade policial, ou em casos específicos pela autoridade judicial, a fim de se preservar os vestígios evitando assim o perecimento dos mesmos.

Portanto a conduta da referida autoridade que antecede ao exame pericial é de fundamental importância para se obter as provas através das perícias.

“ Importante mencionar que entre a iniciativa e a execução do exame pericial há um momento intermediário, referente aos atos preparatórios, consistente na coleta e preservação dos vestígios digitais que possibilitarão a realização do referido exame.” (KERR, 2011, p.59)

Conforme preceitua o artigo 6º do Código de Processo Penal:

> Art. 6º Logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá:
> I - dirigir-se ao local, providenciando para que não se alterem o estado e conservação das coisas, até a chegada dos peritos criminais;
> II -apreender os objetos que tiverem relação com o fato, após liberados pelos peritos criminais;
> III -colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias;
> […]
> VII -determinar, se for o caso, que se proceda a exame de corpo de delito e a quaisquer outras perícias;
> [...]

Entretanto se faz uma crítica quanto aos equipamentos e eventuais vestígios deixados pelos crimes informáticos praticados e que têm relação com o artigo citado acima. Tratam-se de vestígios que envolvem conhecimentos técnicos não somente para a sua análise, mas igualmente para a sua colheita e preservação. Kerr (2011) afirma que somente o especialista em realizar perícias em meios computacionais tem o conhecimento e a competência adequados para executar pessoalmente a coleta, preservação e análise dos vestígios digitais e respectivos equipamentos responsabilizando-se pelos mesmos, sob pena de expor ao risco de alteração, violação ou até destruição dos elementos de prova relacionados.

4.2 Investigação e identificação de autoria

Depois de feita toda a coleta necessária para se comprovar o delito, as autoridades passam pelo processo mais dificultoso e delicado, que é chegar ao autor do crime.

“Existe uma grande mistificação nos dados a serem coletados para se chegar ao verdadeiro autor do crime, devido à fragilidade no conhecimento daqueles que se deparam com uma nova realidade a ser tratada e normatizada. ” (RÉGIS, 2011, p.11)

Para se chegar ao autor do crime há uma burocracia enorme que dificulta o andamento da investigação. Isso se dá pelo endereço IP da máquina do autor que é uma informação protegida pelo sigilo de dados garantido pelo artigo 5º da Constituição Federal. Para se comprovar os dados referentes ao cadastro do IP, faz-se necessária uma autorização judicial para que as autoridades possam acessar as informações referentes ao agente que cometeu o crime pelo computador.

De acordo com Régis (2011, p.11):

> O endereço IP (Internet Protocol) é o número atribuído pelo servidor a toda máquina que se conecta na rede da internet, não só na internet como também em toda e qualquer rede privada e esse número será a informação que identificará onde, quem e quando os indivíduos se conectaram a rede da internet. Tal endereço é a identidade da máquina que está se conectando.

Quando uma máquina acessa à Internet, o servidor de acesso ou o servidor que disponibiliza o acesso à rede atribui um tipo de endereço que servirá de identidade. Este endereço é o IP, representado através de números como, por exemplo, 000.000.000.00. O servidor fornece os dados fundamentais para se chegar ao autor do delito como: hora e data em que foi estabelecida a conexão, número do telefone que solicitou a conexão, nome da máquina etc.

A dificuldade que se dá na investigação das autoridades é principalmente obter as informações necessárias, primordialmente o endereço IP, e consequentemente as outras informações secundárias que poderiam caracterizar como prova.

Depois de obter um número máximo de provas, as autoridades que estão responsáveis pelas investigações devem proceder com uma autorização judicial para quebrar o sigilo do endereço IP.

O processo para a sua obtenção leva cerca de 30 dias e a demora pode comprometer todo o processo de investigação, pois podem ser apagadas ou perdidas devido a sua fragilidade. O indivíduo que pratica o crime pelo computador sabe do papel das provas produzidas contra ele e, para isso, tenta também se livrar o mais rápido possível delas com o intuito de não responderem pelo crime por insuficiência probatória. Afirma Régis (2011, p. 12):

> […] os servidores que armazenam tais informações guardam por pouco tempo em seus bancos de dados, ou seja, as informações de IPs como data, hora, nome da máquina, nome do usuário, e o telefone que solicitou a conexão são perdidos, fazendo assim com que a investigação pare, pois não se têm como chegar ao autor sem tais informações.

Régis (2011, p. 13) afirma que a disponibilização do IP deva se dar de maneira mais fácil porque a própria Constituição Federal veda o anonimato:

> [...] a mais fácil disponibilização do IP para a investigação judicial tem a seu favor o fato de que a Constituição Federal do Brasil veda o anonimato, conforme se afere pelo seu artigo 5º IV - "é livre a manifestação do pensamento, sendo vedado o anonimato"; assim se alguém utiliza a internet como um meio aberto de comunicação, onde pode manifestar suas opiniões e receber as opiniões dos outros, não pode pleitear segredo, pois a CF veda o anonimato nas manifestações de pensamento, e ainda ao se analisar a questão da internet, quando alguém se utiliza de páginas da internet para expor sua vida, para manifestar suas opiniões, para informar-se das opiniões alheias, ou de algum modo observar a vida dos outros, fragiliza-se a alegação de se falar em sigilo de comunicações, já que esta comunicação está sendo feita por um sistema aberto.

Vencida toda a dificuldade relacionada à obtenção do endereçamento IP que está armazenada pelo servidor de Internet é certo dizer que, na maioria dos casos, se chegará ao autor do delito para que esse possa ser responsabilizado pelos seus atos.

4.3 Dificuldade de apuração dos fatos

As provas decorrentes da atividade ilícita nos ambientes virtuais carecem de uma atenção redobrada, pois as mesmas têm um risco de perecimento muito grande e a sua coleta deve ser realizada com bastante cautela. Entretanto, há casos em

que não são deixados vestígios pelos agentes infratores pois os mesmos procuram livrar-se de programas, arquivos, dados ou informações obtidas com a realização da conduta ilícita.

A celeridade e o dinamismo com que esses crimes se propagam na internet, acompanhando o avanço tecnológico que passa a sociedade, acabam trazendo algumas particularidades e barreiras para solução destes delitos. A necessidade de uma perícia especializada, assim como a dificuldade de obtenção da prova de autoria são quesitos que precisam ser avaliados de forma a adaptar-se com o dinamismo que as mudanças tecnológicas proporcionam.

4.3.1 Necessidade de perícias especializadas

Com o crescente aumento da utilização de computadores e da Internet para a prática de crimes, ensejou o surgimento da computação forense para a apuração dos delitos praticados através da rede mundial de computadores.

Toda investigação tem início com base nas evidências e informações coletadas e, no caso dos crimes virtuais, as evidências poderão ser retiradas de qualquer dispositivo eletrônico (celulares, discos rígidos). “A evidência digital pode ser definida como toda informação retirada de um compilado ou depositário eletrônico, através da intervenção humana ou não, em um formato inteligível ao ser humano” (DIAS, 2014, p.32).

Devido a volatilidade de dados e facilidade de adulteração, as provas eletrônicas deverão passar por perícias técnicas rigorosas, de forma a garantir a validade e a integridade dos resultados. A computação forense se encarrega disso: provar os fatos para que fiquem bem claros.

Dias (2014, p.32) afirma que “ A computação forense é a ciência responsável por elucidar os fatos, através da utilização de métodos científicos na coleta, validação, identificação das evidências digitais, para que se possa punir os infratores”. Ela retira o máximo de informações possíveis do delito praticado para que se possa chegar as suas conclusões.

Pelo fato desses crimes se desenvolverem e se consumarem em ambiente virtual, onde não há a presença física do sujeito pois o mesmo se encontra no ambiente cibernético, eles são considerados bastante complexos. Além disso, contribui para essa complexidade a facilidade de perecimento das provas

apresentadas (fotografias, dados, vídeos, arquivos digitais) onde as mesmas podem ser destruídas, perdidas ou modificadas.

Os crimes praticados pelo computador apresentam grandes dificuldades para a sua comprovação em contraste com a facilidade de cometimento dos mesmos. Tais delitos exigem qualificação técnica especifica para a sua apuração quem nem sempre está disponível em todos os lugares de consumação dos crimes.

> A vulnerabilidade de modificação característica dos documentos digitais exige a nomeação de perito tecnicamente qualificado para afirmar a autenticidade do documento. Apesar da precisão da computação forense, a coleta de evidências se torna frágil. Quando feita erroneamente, violando disposições de direito material ou princípios constitucionais, pode tornar a prova ilícita ou invalidá-la. (DIAS, 2014, p.33)

Em decorrência desse tipo de perícia, o maior problema na produção de provas referentes aos crimes virtuais é o despreparo da polícia investigativa e da perícia. O número de profissionais preparados para esse tipo de investigação é pouco e, por isso, estes deverão ser extremamente capacitados e especializados para lidar com a perícia voltada para a investigação dos crimes digitais, de forma a atender certas exigências técnicas de coleta e guarda para se evitar questionamentos sobre a licitude do material obtido (COLLI, 2010).

Com a finalidade de dar veracidade às provas produzidas, a investigação criminal e a instrução processual demandam procedimentos técnicos. Os profissionais que têm especialidade em *hardware*, *software*, tráfego e segurança de rede, com os exames periciais, ficarão encarregados de buscar a verdade dos fatos. A eficiência da investigação criminal é fruto do trabalho dos peritos na análise de onde ocorreram os fatos e na procedência deles (DIAS, 2014, p. 34).

Diante da necessidade de especialização dos responsáveis que investigam os crimes informáticos, Colli (2010) afirma que criar divisões especializadas em computadores, mídias e meios de comunicação poderia ser uma das vias para o combate de questões relacionadas aos delitos praticados pelo computador. Isso viabilizaria uma agilidade maior dos profissionais técnicos para a apuração dos fatos já que a velocidade e novidade das práticas delituosas ensejam um conhecimento específico para que se possa chegar ao autor do delito.

> Embora o país esteja se preparando para o combate aos crimes virtuais, através da criação de delegacias especializadas e do treinamento de

> profissionais responsáveis por investigar tais crimes, a quantidade de profissionais dessa área não é suficiente para apurar as condutas ilícitas praticadas diariamente na rede mundial de computadores. Na sociedade atual a qual a tecnologia se faz presente no cotidiano das pessoas, inclusive em momentos de práticas criminosas, o papel do perito computacional, responsável por desvendar e solucionar crimes que necessitam de um conhecimento específico, é de extrema importância. (QUEIROZ; VARGAS, 2010, p.10 apud DIAS, 2014, p.35)

4.3.2 Problema na identificação de autoria

Para que haja a sanção penal ao indivíduo imputado, é preciso a comprovação de que o mesmo tenha realizado a conduta definida como um crime informático. Não basta a dedução, inferência ou conhecimento raso sobre a autoria do delito (DIAS, 2014).

Primordialmente se tratando dos crimes virtuais, a exata identificação do agente delituoso se trata de um empecilho preocupante para que a pretensão punitiva seja justa e focada naquele que realmente cometeu o delito informático. Essa preocupação é ainda maior, em relação a identificação do autor, quando se considera, por exemplo, a facilidade que os criminosos têm em invadir sistemas e a apropriação e uso indevido de senhas de acesso alheias para a prática de golpes financeiros.

> Quando a imputação do crime virtual é determinada somente através da simples indicação do possível autor que cometeu o ilícito penal, não poderá ser instaurado um juízo. A individualização do autor da infração penal, sua correta identificação e qualificação, é pressuposto essencial para a instauração da instrução processual penal. (MALAQUIAS, 2012, p.64 apud DIAS, 2014, p. 37)

Pode-se dizer que uma das características dos crimes praticados pelo computador é o anonimato on-line, pois o ambiente em que eles são praticados não apresenta um espaço físico, concreto. Os agentes delituosos passam a assumir qualquer identidade que queiram adotando técnicas que escondam sua verdadeira identificação.

Entretanto, ao se considerar a identificação do computador, este conceito de anonimato fica relativizado. Isso acontece pela atribuição de um endereço IP que permitirá a atribuição de identidade a qualquer máquina que se conecte a rede mundial de computadores.

> Toda investigação criminal deve considerar as evidências deixadas pelo criminoso cibernético por intermédio do endereço IP. Outra forma de se obter informações de acesso à rede é através do servidor proxy, responsável por armazenar os logs de registro de navegação que identificam os locais acessados pelo usuário, bem como os serviços utilizados, quando a conexão com a rede mundial de computadores é direta. Apesar dessas duas hipóteses investigativas, não há como fazer esse rastreamento, quando o usuário se conecta à rede através de uma conexão indireta, pela qual o internauta fica protegido e usufrui do anonimato on-line para acessar vários conteúdos, utilizando apenas o IP do servidor hospedeiro. (MALAQUIAS, 2012, p.65 apud DIAS, 2014, p.38)

Portanto, a toda máquina que se conecta à rede é atribuído um número de identificação, o IP, que permite a localização da pessoa no mundo virtual. Contudo, não se pode determinar com certeza a autoria pois a identificação é sempre do computador, e não do sujeito que cometeu a prática delitiva.

Dias (2014) afirma que a grande dificuldade decorrente da identificação de autoria está em correlacionar o computador com o sujeito que efetivamente o operou. Um computador de uso público como o de Universidade, *lan-house* ou biblioteca, por exemplo, pode ser utilizado por vários indivíduos e isso dificulta o trabalho da perícia em imputar a prática do delito ao verdadeiro criminoso informático.

Peck (2013, p.93) apud Dias (2014, p. 40) afirma que a questão da prova de autoria é um dos grandes desafios do direito na era digital e a identificação do criminoso, de maneira inequívoca, só é possível através de biometria, se utilizando de características como reconhecimento fácil e a impressão digital.

Peck (2013, p.93 apud DIAS, 2014, p.40) ainda cita a participação do juiz no entendimento da autoria de crime cibernético:

> O tema da identidade digital obrigatória pode ser considerado como um dos assuntos mais importantes do direito atual. A ausência de uma lei para gerar prova de autoria e de um entendimento consolidado e unificado incorre em várias possibilidades de entendimento por parte do juiz quando se depara com um crime cibernético. Há juiz que entende que a senha é suficiente para comprovação da identidade do autor, outros aplicam isso apenas quando há o certificado digital da ICP-Brasil, e há ainda os que dizem que só com a assinatura do papel.

Portanto, a única forma segura de identificação do autor de delito informático é aquela que leva em consideração a análise do infrator penal, quando este se utiliza de elementos corporais para acessar o ambiente virtual. Assim, haverá a individualização do mesmo não havendo dúvida quanto a autoria do crime.

5 CONCLUSÃO

A presente monografia teve como objetivo analisar os principais crimes informáticos na ótica do Direito brasileiro, demonstrando as suas peculiaridades quanto a dificuldade na apuração dos fatos pela investigação criminal. A recente tipificação de algumas condutas ainda não é suficiente para solucionar a problemática em torno da solução de tais delitos.

Os avanços tecnológicos e a popularização da Internet fizeram com que esse meio de comunicação se tornasse indispensável na vida cotidiana de cada indivíduo. A internet, além de ser o meio de comunicação principal no mundo moderno, se

tornou o ambiente da prática de delitos já tipificados na legislação penal, bem como permitiu o surgimento de crimes cujos os bens jurídicos são as informações, dados e sistemas de computador.

A constituição da prova, no Direito, é um instituto importante para a averiguação da verdade. Com ela, deverão ser colhidos dados, informações e as partes envolvidas terão que demonstrar os fatos e não simplesmente alegá-los, já que a prova é instrumento que serve para o convencimento do juiz no processo.

Quando se fala dos crimes virtuais e suas características, deve-se levar em consideração a efemeridade e a volatilidade dos dados transmitidos e armazenados nos computadores que podem levar a dificuldade do seu processo de investigação. Uma solução para evitar este empecilho e assegurar a integridade das provas, bem como adequar a velocidade das unidades policiais à velocidade dos crimes cibernéticos, seria a investigação por meio de divisões especializadas neste tipo de crime.

Em um processo investigativo, a admissão e coleta das provas são elementos indispensáveis para se chegar à autoria do delito. Os meios tecnológicos na prática dos crimes virtuais dificultam a obtenção da prova, sendo necessário a atuação de um perito que irá extraí-las e garantirão a autenticidade de certos documentos.

Quando se fala do autor do crime de informática tem-se logo a dificuldade para a sua identificação. A individualização do acusado, levando-se em conta sua identidade e qualificações, é um problema muito constante para as autoridades devido ao anonimato proporcionado pelo ambiente em que as condutas delituosas são praticadas, onde não há a presença de um espaço físico. Mesmo que seja possível identificar a máquina de onde foi praticada o delito, os peritos ainda terão o trabalho de associar o proprietário do computador com o sujeito que praticou o crime.

Umas das soluções para se chegar ao autor do delito, já que há a dificuldade para associar o computador de onde foi cometido o crime ao agente, é a utilização de biometria ou qualquer outro meio que possibilite a identificação fisiológica do usuário da rede virtual. Outro meio seria a responsabilização do acusado se houvesse somente a prisão em flagrante com o equipamento ligado, o que não restaria dúvidas para as autoridades policiais quanto à autoria.

Em decorrência de suas características, efemeridade e volatilidade, a comprovação dos crimes virtuais é muito difícil. A dificuldade probatória e a

facilidade no encobrimento de dados demandam que a realização das provas nesse tipo de crime ocorra em um curto período de tempo, de forma a evitar que alguns dados essenciais para a comprovação do delito sejam perdidos. Por esse motivo, a investigação dos crimes virtuais está intimamente ligada à necessidade da produção antecipada de provas, previsto no Código de Processo Penal como uma medida excepcional a ser utilizada somente em casos relevantes quando não for possível a repetição em juízo, sempre observando a garantia do contraditório e da ampla defesa.

Conclui-se, então, que os crimes de informática estão ocorrendo com mais frequência à medida que as tecnologias evoluem. Tais delitos são caracterizados pela dificuldade na obtenção de provas e na atribuição de autoria, pois os dados que fornecerão de embasamento para a investigação dos peritos são efêmeros e voláteis. A utilização da biometria e a prisão em flagrante com o computador operante seriam opções para solucionar tal problema e o instituto da produção antecipada de provas ganha importância nesse contexto diante da possibilidade de perecimento das mesmas.

REFERÊNCIAS

Ao chantagear vítima exigindo pornografia, homem é preso por estupro virtual. **Revista Consultor Jurídico** (internet), 11 de agosto de 2017. Disponível em:< http://www.conjur.com.br/2017-ago-11/exigir-pornografia-vitima-homem-preso-estupro-virtual>. Acesso em: 15 de agosto de 2017.

ARANHA, A.J.Q.T.C. **Da prova no processo penal**. 3. ed. atual. São Paulo: Saraiva, 1994.

ARAÚJO, André Ferreira de. **A dificuldade de apuração dos crimes de pedofilia cometidos através da internet**. Disponível em

<http://www.webartigos.com/artigos/a-dificuldade-de-apuracao-dos-crimes-de-pedofilia-cometidos-atraves-da-internet/91222/>. Acesso em: 20 de julho de 2017.

ASSUNÇÃO, Marco Flávio Araújo. **Segredos do Hacker Ético**.2ª ed. Visual Books: Florianópolis, 2008.

BARROS, Marco Antônio. **A busca da verdade no processo penal**. São Paulo: Editora Revista dos Tribunais, 2011.

BASSO, Maristela; POLIDO, Fabrício. **Jurisdição e Lei Aplicável na Internet: Adjudicando litígios de violação de direitos da personalidade e as redes de relacionamento social**. In: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) Direito & Internet: Aspectos Jurídicos Relevantes. v. 2. São Paulo: Quartier Latin, 2008.

BIASOLI, Luiz Carlos de Sales. **Da necessidade de tipificação do crime de estelionato praticado na internet**. 2010. Disponível em: <http://www.conteudojuridico.com.br/monografia-tcc-tese,da-necessidade-de-tipificacao-do-crime-de-estelionato-praticado-na-internet,25896.html>. Acesso em: 28 de julho de 2017.

BRASIL. **Constituição Federal de 1988**. Promulgada em 5 de outubro de 1988. Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/constituição.htm>. Acesso em: 28 de julho de 2017.
BRASIL. **Decreto-Lei nº 2.848 de 7 de dezembro de 1940**. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848compilado.htm>. Acesso em: 20 de julho de 2017.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm>. Acesso em: 28 de julho de 2017.

BRASIL. **Lei n. 12737, 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. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 24 de julho de 2017.

BRASIL. **Lei n. 9296, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9296.htm>. Acesso em: 29 de julho de 2017.

BRASIL. **Lei n. 9609, de 19 de fevereiro de 1998**. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9609.htm>. Acesso em: 28 de julho de 2017.

BULOS, Uadi Lammego. **Constituição Federal anotada.** 5. ed. São Paulo: Saraiva, 2003.

CARDOSO, Daiene. Câmara aprova projeto que torna crime divulgação de 'nudes' na internet. **O Estado de S. Paulo**, São Paulo, 21 de fevereiro de 2017. Disponível em:< http://brasil.estadao.com.br/noticias/geral,camara-aprova-projeto-que-torna-crime-divulgacao-nudes-na-internet,70001674551>. Acesso em:15 de agosto de 2017.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus aspectos Processuais**. 2. ed. Rio de Janeiro: Lumen Juris, 2003.

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

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

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-informativos-gisele-truzzi-alexandre-daoun.pdf>. Acesso em: 20 de julho de 2017.

DIAS, Camila Barreto Andrade. **Crimes virtuais: as inovações jurídicas decorrentes da evolução tecnológica que atingem a produção de provas no processo penal**. Disponível em:< http://www.egov.ufsc.br/portal/sites/default/files/20888860.pdf>. Acesso em: 31 de julho de 2017.

FERREIRA, Ivette Senise. **A Criminalidade Informática. In: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) Direito & Internet: Aspectos Jurídicos Relevantes**. 2. ed. São Paulo: Quartier Latin, 2005.

FERREIRA, Lóren Formiga de Pinto. **Os "crimes de informática" no Direito Penal Brasileiro**. In: **Âmbito Jurídico**, Rio Grande, XII, n. 63, abril de 2009. Disponível em:<http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=6064>. Acesso em jul 2017.

FILHO TOURINHO, Fernando da Costa. **Manual de Processo Penal***.* São Paulo: Saraiva, 2009.

FINKELSTEIN, Maria Eugênia. **Fraude Eletrônica. In: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) Direito & Internet: Aspectos Jurídicos Relevantes**.2 v. São Paulo: Quartier Latin, 2008.

FONTES, Edison. **Segurança da Informação: O usuário faz a diferença**. São Paulo: Saraiva, 2006.

GALDEMANN, Henrique. **De Gutemberg à Internet: Direitos autorais na era digital**. 4. ed. Rio de Janeiro: Record, 2001

GRECO, Rogério. **Código Penal: Comentado/ Rogério Greco** – 4 ed. – Niterói, RJ: Impetus. 2010
.
JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos- Ameaças e procedimentos de investigação**. Rio de Janeiro: Braspot, 2012.

KERR, Vera Kaiser Sanches. **A disciplina, pela legislação processual penal brasileira, da prova pericial relacionada ao crime informático praticado por meio da internet**. Vera Kaiser Sanches Kerr. - ed. Ver. –São Paulo, 2011. 135p. Disponível em: <http://bdtd.ibict.br/vufind/Record/USP_90d39d3b76f8dfbff0c3b565364ac9bc>. Acesso em: 20 de julho de 2017.

LEITE FILHO, Jaime de Carvalho. **Ciberterrorismo – O Terrorismo na Era da Informação**. In: ROVER, Aires José Direito e Informática. Barueri: Manole, 2004.

LIMA, Antonio Henrique Maia**. Crimes de internet: da competência e da dificuldade de obtenção de provas no meio eletrônico**. In: Âmbito Jurídico, Rio Grande, XVII, n. 127, ago 2014. Disponível em: <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=14253>. Acesso em: 24 de julho 2017.

MALAQUIAS, Roberto Antônio Darós. **Crime Cibernético e Prova – A investigação criminal em busca da verdade**. Curitiba: Juruá Editora, 2012.
MATOS, Mariana Maria. **Da produção e colheita de provas no ambiente cibernético**. 2014. Disponível em: <https://marianamariam.jusbrasil.com.br/artigos/119753698/da-producao-e-colheita-de-provas-no-ambiente-cibernetico>. Acesso em: 24 de julho de 2017.

Ministério Público Federal. **Crimes Cibernéticos:** manual prático de investigação. São Paulo, 2006. Disponível em:<http://www.mpdft.gov.br/portal/pdf/unidades/promotorias/pdij/TAC/Manual_de_Crimes_de__Inform%C3%A1tica_-_vers%C3%A3o_final2.pdf>. Acesso em: 20 de julho de 2017.

MIRABETE, Julio Fabbrini. **Código Penal Interpretado**. 3. ed. São Paulo: Atlas, 2003.

MORAES, Alexandre de. **Direitos Humanos Fundamentais: teoria geral, comentários aos arts. 1º a 5º da Constituição da República Federativa do Brasil, doutrina e jurisprudência**. 8. ed. São Paulo: Atlas, 2007.

MORAES, Alexandre de. **Direito Constitucional***.* São Paulo: Editora Atlas, 2010.

MOTTA, Carlos. **Princípios da Proteção Negocial e Jurídica para Empreendedores em Tecnologia**. In: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) Direito & Internet: Aspectos Jurídicos Relevantes. v. 2. São Paulo: Quartier Latin, 2008.

MUOIO, Arlete Figueiredo; AGUIAR, Malu. **Crimes na Rede: o perigo que se esconde no computador**. São Paulo: Companhia Limitada, 2006.

NETO, Pedro Americo de Souza. **Crimes de Internet**. 2009. 81 p. Monografia (Bacharelado em Direito) - UNIVALI, Vale do Itajai, 2009. Disponível em: <http://siaibib01.univali.br/pdf/Pedro%20Americo%20de%20Souza%20Neto.pdf>. Acesso em: 17 jul. 2017.

NOGUEIRA, Sandro D'Amato. **Crimes de informática.** 2. ed. São Paulo: BH Editora e Distribuidora, 2009.

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

PIRAGIBE, Clélia. **Indústria da Informática:** Desenvolvimento Brasileiro e Mundial. Rio de Janeiro: Campus, 1985.

PRADO, Luiz Regis. **Direito penal: Parte Especial – arts. 121 a 196. 2. ed. reform., atual. e ampl**. São Paulo: Revista dos Tribunais, 2008.

RÉGIS, André Tavares. **Crimes contra a honra na internet: dificuldade na apuração dos fatos**. Disponível em: <http://www.fespfaculdades.com.br/painel/uploads/arquivos/TCC%20ANDRE%20TAVARES%20REGIS.pdf>. Acesso em: 20 de julho de 2017.

ROSA, Fabrízio. **Crimes de Informática**. 2.ed. Campinas: BookSeller, 2006.
ROSSINI, Augusto Eduardo de Souza. **Brevíssimas considerações sobre delitos informáticos.** Caderno Jurídico**,** São Paulo, n. 4, ano 2, jul. 2002.

RUFINO, Nelson Murilo de O. **Segurança Nacional: Técnicas e Ferramentas de Ataque e Defesa de Redes de Computadores**. São Paulo: Novatec, 2002.

SANTA CRUZ, Frank Ned. **PL 5.555/13 – Lei Rose Leonel**. Disponível em:< http://www.migalhas.com.br/dePeso/16,MI254877,101048-PL+555513+Lei+Rose+Leonel>. Acesso em: 15 de agosto de 2017.

SÃO PAULO. Tribunal de Justiça de São Paulo. **Apelação nº 1023474-16.2014.8.26.0576, da 35º Câmara de Direito Privado do Tribunal de Justiça de São Paulo**. São Paulo, SP, 2 de maio de 2017. Disponível em: <https://tj-sp.jusbrasil.com.br/jurisprudencia/455637994/apelacao-apl-10234741620148260576-sp-1023474-1620148260576?ref=juris-tabs>. Acesso em 28 de julho de 2017.

TAMEGA, Flávio. **Hacker Inside.v.1**. Goiânia: Editora Terra, 2003.

TATEOKI, Victor Augusto**. Classificação dos Crimes Digitais**. Disponível em:<https://victortateoki.jusbrasil.com.br/artigos/307254758/classificacao-dos-crimes-digitais>. Acesso em: 26 de julho de 2017.

TEIXEIRA, Tarcisio. **Curso de direito e processo eletrônico: doutrina, jurisprudência e prática**. São Paulo: Saraiva, 2014.

TELES, Ney Moura. **Direito penal: Parte Especial: arts. 121 a 212, v. 2**. São Paulo: Atlas, 2004.

TORRES, GABRIEL. **Redes de Computadores Curso Completo**. Rio de Janeiro: Axel Books, 2001.

VIANA, Túlio Lima**. Do delito de dano e de sua aplicação ao direito penal informático**. Revista dos Tribunais, São Paulo, a. 92, v. 807, 2003.

VIANA, Tulio; MACHADO, Felipe. **Crimes informáticos**. Belo Horizonte: Fórum, 2013.

WACHOWICZ, Marcos. **O Programa de Computador como Objeto do Direito Informático**. In: ROVER, Aires José Direito e Informática. Barueri: Manole, 2004.

WENDT, Emerson.; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport, 2012.