AJES – FACULDADE DE CIÊNCIAS CONTÁBEIS E ADMINISTRAÇÃO DO VALE DO JURUENA

BACHARELADO EM DIREITO

ADRIANO LUIZ HERMES

O PROBLEMA DA PERSECUÇÃO CRIMINAL NOS DELITOS INFORMÁTICOS: DA ANÁLISE DAS PROVAS

JUÍNA-MT

2013

AJES – FACULDADE DE CIÊNCIAS CONTÁBEIS E ADMINISTRAÇÃO DO VALE DO JURUENA

BACHARELADO EM DIREITO

ADRIANO LUIZ HERMES

O PROBLEMA DA PERSECUÇÃO CRIMINAL NOS DELITOS INFORMÁTICOS: DA ANÁLISE DAS PROVAS

"Monografia apresentada ao curso de Bacharelado em Direito, da Faculdade de Ciências Contábeis e Administração do Vale do Juruena como requisito parcial para obtenção do título Bacharel em Direito".

Orientador: Guilherme Augusto Pinto da Silva

JUÍNA-MT

2013

AJES – FACULDADE DE CIÊNCIAS CONTÁBEIS E ADMINISTRAÇÃO DO VALE DO JURUENA

CURSO: BACHARELADO EM DIREITO

BANCA EXAMINADORA

Orientador: Professor Mestre Guilherme Augusto da Silva

Presidente da Banca

Professor Mestre Afonso Mª das Chagas

Membro

Professora Mestre Patrícia Fernandes Fraga

Membro

AGRADECIMENTOS

Agradeço a Deus,
Aos familiares e amigos que me deram forças.
Ao meu orientador e a todos os professores,
que durante o curso contribuíram para esta conquista.

Dedico a todos que de alguma forma contribuíram para que eu chegasse aqui, aos amigos, que sempre estiveram a meu lado.

Minha irmã, Leandra, que

sempre deu incondicional apoio.

Em especial a minha querida mãe,

que mesmo diante das dificuldades,

me ensinou da melhor forma,

através de bons exemplos.

"Teu dever é lutar pelo Direito,
mas se um dia encontrares o Direito
em conflito com a Justiça,
luta pela Justiça"

(Eduardo Juan Couture)

RESUMO

Desde o descobrimento do fogo o homem iniciou uma busca incessante por criar meios de facilitar sua vida sobre a terra. Passou então a domesticar animais e cultivar alimentos, construir ferramentas que os auxiliassem nos serviços manuais. Posteriormente, em um momento conhecido como Revolução Industrial, inventou máquinas movidas a vapor que substituíam grande parte da mão de obra humana. Assim, no anseio por novas descobertas e tecnologias, surgiram os primeiros computadores, fase esta da sociedade, que para muitos autores pode ser denominada como uma segunda revolução industrial, uma vez que substituiu o trabalho intelectual do homem pelo trabalho de máquinas capazes de processar dados e gerar informações. Inúmeros são os benefícios trazidos com o advento dos computadores, sendo que, pode-se destacar a facilidade da comunicação entre distâncias, avanços na medicina, dentre outros. Porém, o advento desta tecnologia trouxe consigo novos meios de praticar condutas já tipificadas como crimes, bem como novos atos ilícitos, os quais só podem ser cometidos através de sistemas digitais. Assim, levando em conta que o direito tem por escopo assegurar a aplicação da justiça, deve também evoluir, para que possa acompanhar os novos conceitos, as novas culturas da atual sociedade globalizada. Com advento de novos meios de cometer crimes, ou mesmo, com o surgimento de novos delitos, cabe ao direito tutelar o bem jurídico objeto do ato criminoso, bem como especificar o modo como ocorrerá a persecução criminal, especialmente no que diz respeito à análise das provas, que, no ambiente virtual encontra-se adstrita a várias peculiaridades.

Palavras-Chave: Delitos Informáticos; crime; virtual; computador; prova; persecução criminal.

ABSTRACT

Since the discovery of fire the man began a relentless pursuit to create ways to facilitate your life on earth . Then began to domesticate animals and grow food , build tools that should assist in the service manuals . Later, in a time known as the Industrial Revolution , invented steam engines that replaced much of human labor . Thus , the desire for new discoveries and technologies , were the first computers , this phase of society , which for many authors can be referred to as a second industrial revolution , since replaced the intellectual work of man by the work of machines capable of processing data and generate information . There are countless benefits brought by the advent of computers , and that can highlight the ease of communication between distances , advances in medicine , among others . However , the advent of this technology has brought new ways of practicing behaviors have typified as crimes , as well as new unlawful acts , which can only be committed through digital systems . Thus , taking into account that the right is to ensure the application scope of justice , must also evolve , so you can keep up with new concepts , new cultures present globalized society . With the advent of new ways of committing crimes , or even with the emergence of new offenses , it is the law protect the legal object of criminal act , as well as specify how the criminal prosecution occur , especially with regard to the analysis of evidence that the virtual environment is circumscribed to several peculiarities .

Keywords: Computer crimes, crime, virtual computer; evidence; criminal prosecution.

SUMÁRIO

INTRODUÇÃO

Desde os primeiros delitos praticados na história, sempre houve alguém ou um determinado grupo de pessoas responsáveis por realizar justiça, isto é, aplicar ao agente que cometeu o ato criminoso, uma sanção, proporcional a seu ato injusto, de forma que, o criminoso entenda a gravidade de sua conduta, bem como sinta a reprovação da sociedade, diante de sua ação.

Todavia, para aplicar tal punição, necessário se faz ter a certeza quanto à autoria e materialidade do ato criminoso, isto é, verificar, se realmente houve o crime e se o acusado realmente foi o responsável por tal ato, pelo que, existe a persecução criminal, que pode ser dividida em duas fases, a inquisitorial, realizada na esfera administrativa e a judicial que é de competência do poder judiciário.

Em ambas as fases, para alcançar os dois objetos – autoria e materialidade – serão colhidas provas, o que darão ao julgador a convicção quanto à aplicação de uma pena, ou não, ao acusado. Porém para realizar a colheita dessas provas, há que se verificar algumas peculiaridades, principalmente nos delitos informáticos, objeto desta pesquisa.

A fim de esclarecer questões referentes à validade das provas nos delitos informáticos, serão apresentadas algumas espécies desses crimes, de forma a tornar compreensível a persecução criminal nesses delitos, abarcando principalmente a matéria concernente às provas.

Serão demonstrados pontos em que os delitos informáticos diferem dos demais crimes, especialmente no que concerne a produção de provas, considerando à inviolabilidade do sigilo à correspondência e das comunicações telegráficas, de dados, dentre outros, os quais estão previstos na Constituição Federal.

Ainda serão abordas algumas das dificuldades encontradas pelos profissionais responsáveis pela realização da persecução criminal, a falta de legislação específica para punir os criminosos que cometem delitos informáticos.

Desse modo, serão pontuados alguns momentos históricos, tidos como marcos, para evolução da informática, fazendo uma breve análise história, quanto às mudanças ocorridas na sociedade, desde a evolução industrial, com a criação de máquinas que realizam trabalhos que antes eram manufaturados, até a era da informação, quando as máquinas, além dos trabalhos físicos (braçais), passaram a efetuar trabalho intelectual.

Máquinas inteligentes passaram a integrar a sociedade tomando espaço no dia a dia das pessoas e tornando cada vez mais irreversível a necessidade do uso destes equipamentos e,

com o aumento do número de pessoas utilizando computadores após o advento da internet, constatou-se também um grande número de pessoas mal intencionadas neste ambiente, que encontraram no meio digital uma forma “segura” de cometer crimes, dificultando a obtenção de provas.

Na presente pesquisa, far-se-á um apanhado geral dos delitos informáticos, iniciando-se com a parte histórica e conceituação, realizando-se, ainda que de forma sucinta, uma abordagem dos delitos informáticos, no segundo capítulo, especificar-se-á a divisão entre os delitos informáticos próprios e impróprios, por fim, no terceiro e último capítulo será feita a conceituação de prova e a forma como ela é analisada nos delitos informáticos, principalmente em relação à dificuldade de obtenção e questão do sigilo de dados, previsto na Constituição Federal, ainda, serão apresentadas algumas das principais dificuldades encontradas pelos responsáveis pela persecução criminal dos delitos informáticos.

CAPÍTULO. I. DELITOS INFORMÁTICOS, SURGIMENTO E CONCEITO

O crime é algo tão antigo quanto a própria existência da humanidade e uma das principais razões da existência do direito é justamente dirimir os impasses oriundos da prática dos crimes.

Com a evolução da sociedade, evoluem também as formas e os meios de praticar crimes, restando ao direito o dever de acompanhar essa evolução, cabendo ao poder legislativo acompanhar as evoluções tecnológicas reconhecidamente implementadas na sociedade. Diante da velocidade com que evoluem os equipamentos eletrônicos e softwares, novas práticas delitivas surgem, sem que haja tipificação ou diagnóstico jurídico do problema enfrentado.

1.1 – Histórico

Toda a tecnologia que se tem hoje deve-se ao esforço do homem em desenvolver máquinas e ferramentas que facilitem seu trabalho, partindo da fabricação de ferramentas rudimentares na pré-história até a criação de microprocessadores capazes de realizar façanhas inimagináveis há pouco mais de cinquenta anos, o que, para os interpretes do direito resultou significativas mudanças, principalmente no que diz respeito à forma de praticar os crimes.

Importante fator que influenciou de forma determinante a corrida tecnológica foi a Revolução Industrial, que se caracteriza pela série de mudanças iniciadas na Inglaterra e que se espalharam pela Europa nos séculos XVIII e XIX, tendo como principal característica a substituição do trabalho que antes era feito de forma artesanal pelo trabalho assalariado. Essa implementação se deu principalmente com o uso de máquinas, quando surgiam as linhas de produção e os trabalhadores que antes faziam todo o trabalho artesanalmente agora realizavam apenas parte de um processo de produção[1].

Grandes invenções foram verificadas a partir deste período, dentre elas, pode-se destacar a fotografia em 1839, pelo pintor e físico francês Louis Daguerre, o telefone em 1876 pelo escocês Alexandre Graham Bell, a luz elétrica em 1879 que se deu com o desenvolvimento da lâmpada incandescente pelo americano Thomas Edison, o carro em 1886 pelo engenheiro

[1] BASE DE DADOS PORTAL DO BRASIL. **Historia Geral: Revolução Industrial**. Disponível em <http://www.portalbrasil.net/historiageral_revolucaoindustrial.htm>. Acesso em 04/03/2013.

alemão Gottlieb Daimler, o rádio em 1896, criado pelo italiano Guglielmo Marconi, o computador em 1945, o satélite em 1957 e a internet em 1969[2].

Atualmente, atravessa-se uma era denominada "Era da Informação", que tem seu início após a Era Industrial, destacando-se a partir da década de 1970, com o advento dos microprocessadores, dos computadores interligados, bem como da fibra ótica e computadores de uso pessoal[3].

Devido a evolução do homem e a busca incansável pela criação de novas tecnologias que auxiliem e facilitem sua vida, tem-se uma sociedade que muda rapidamente, em que as informações são transmitidas de forma cada vez mais veloz. Nesse sentido, vários são os benefícios trazidos pela tecnologia, como a facilitação da comunicação entre pessoas que encontram-se geograficamente longe uma das outras e o comércio entre distâncias continentais, dentre outros inúmeros benefícios. Verifica-se que a evolução tecnológica também traz problemas, tendo em vista a popularização da rede mundial de computadores, o que facilita a inserção de pessoas mal intencionadas neste meio.

Necessário se faz esclarecer como e porque se deu a popularização do computador[4] e do acesso à internet[5].

A necessidade de realização de cálculos precisos e eficientes resultou no surgimento do *Eletronic Numerical Integrator and Computer*, ou ENIAC, o primeiro computador, construído com válvulas eletrônicas.

> O ENIAC era mil vezes mais rápido que qualquer máquina anterior, resolvendo 5 mil adições, 350 multiplicações ou 50 divisões por segundo. (...) Encheu 40 gabinetes com 100 mil componentes, incluindo cerca de 17 mil válvulas eletrônicas. Pesava 27 toneladas e media 5,50 x 24,40 m.[6]

---

[2] PANIZO, Francisco. NET ALMANAQUE. **Invenções que mudaram o mundo e sobreviveram ao tempo**. Disponível em: <http://www.superdicas.com.br/almanaque/almanaque.asp?u_action=display&u_log=254>. Acesso em: 04 mar. 2013.

[3] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1 ed. 2ª tiragem, Saraiva: 2011: São Paulo. p. 25.

[4] Cf. Dicionário Aurélio Eletrônico de 2010: computador é a "máquina capaz de receber, armazenar e enviar dados, e de efetuar, sobre estes, seqüências previamente programadas de operações aritméticas (como cálculos) e lógicas (como comparações), com o objetivo de resolver problemas".

[5] Cf. Dicionário Aurélio Eletrônico 2010: "Qualquer conjunto de redes de computadores ligadas entre si por roteadores e *gateways*, como, p. ex., aquela de âmbito mundial, descentralizada e de acesso público, cujos principais serviços oferecidos são o correio eletrônico (q. v.), o *chat* (q. v.) e a *Web* (q. v.), e que é constituída por um conjunto de redes de computadores interconectadas por roteadores que utilizam o protocolo de transmissão TCP/IP."

[6] ABRIL, Editora. **A Era do Computador, Ciência & Natureza**. Abril Livros: Rio de Janeiro, 2010. p. 14.

Outro grande passo foi dado pela empresa Xerox que lançou no ano de 1991 o primeiro computador com *mouse* e interface gráfica. No ano seguinte a Intel pôs no mercado o primeiro computador pessoal[7].

Desde a criação do ENIAC em 1946 os computadores passaram por muitas mudanças, com inovações em espaços de tempo cada vez menores, realizando outras tarefas além de apenas cálculos. Consequentemente os computadores popularizaram-se e passaram a integrar o cotidiano do homem, diminuíram de tamanho e aumentaram a funcionalidade, sendo integrados em várias ações do cotidiano.

Igualmente, o que impulsionou a popularização dos computadores pessoais foi a criação da internet, meio encontrado para interligar computadores de todo o mundo, através de uma rede descentralizada.

Sua origem data da década de 60 e resultou da união de algumas universidades que tinham por objetivo desenvolver a ARPANET (Advanced Research Projects Administration), seu uso era restrito das Forças Armadas Norte Americanas e tinha por escopo construir um sistema de comunicação que fosse resistente até mesmo a um ataque nuclear, ou seja, uma forma de comunicação que não dependesse de um sistema central que poderia ser atingido e destruído, reflexo causado devido ao medo imposto pela guerra fria naquela época.[8]

A ARPANET evoluiu e com a implementação do Protocolo de Controle de Transferência/Protocolo de Internet (TCP/IP – *Internet Protocol*) deu-se origem a internet, este protocolo possibilita a interligação de vários computadores em rede, tornando possível que atuem em grupo[9].

Apesar do tempo decorrido a ideia principal do funcionamento da internet é a mesma, eis que se baseia no princípio de que não há um ponto central, ou seja, não existe um servidor que em caso de destruição toda a rede deixará de funcionar. A rede é formada de todos os dispositivos a ela conectados, de forma que, caso deixe de funcionar um determinado ponto, apenas ele deixará de existir, a internet continuará operando normalmente.

Todavia, esta facilidade em integrar o mundo das informações que viajam na velocidade da luz, ou seja, a disseminação dos computadores e da internet afeta diretamente o cotidiano das pessoas. Vive-se em uma era em que há possibilidade de se fazer praticamente tudo *on line*, pode-se fazer compras, visitar museus, conhecer lugares, encontrar pessoas, até

---

[7] PINHEIRO, Patrícia Peck. **Direito Digital.** 4 ed. Saraiva: São Paulo, 2010. p. 58.
[8]KLEINA, Nilton. **A História da Internet: Pré-década de 60 até anos 80**. TECMUNDO, disponível em <http://www.tecmundo.com.br/infografico/9847-a-historia-da-internet-pre-decada-de-60-ate-anos-80-infografico-.htm>, acesso em 26/10/2013.
[9] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1 ed. 2ª tiragem, Saraiva: São Paulo, 2011. p. 30.

mesmo consultas médicas, enfim, uma infinidade de coisas que há pouco mais de 50 anos atrás não era possível se imaginar fazer de outra forma senão que pessoalmente, porém isto cria uma nova rotina para as pessoas, bem como uma nova cultura, modificando a forma de pensar e até mesmo os valores de cada indivíduo, surgindo assim, uma nova sociedade, a sociedade da informação.

1.2 - Sociedade da informação

A *Sociedade da Informação* é fruto de um processo lento. Em um sentido amplo, tem sua origem na revolução industrial quando houve a substituição do trabalho físico de animais e homens pelo trabalho de máquinas. Posteriormente com o surgimento dos computadores, houve a substituição do trabalho intelectual do homem pela máquina. Ainda, segundo alguns sociólogos e economistas a passagem da sociedade industrial para a sociedade da informação foi uma *segunda revolução industrial*[10].

Em todo o mundo o número de pessoas com acesso a internet cresce em larga escala. Segundo o IBOPE, somente no Brasil, no segundo trimestre de 2012 o total de pessoas com acesso a internet foi de 94,2 milhões[11]. Um número que cresce consideravelmente rápido, principalmente tendo em vista o baixo custo e as facilidades de adquirir um dispositivo com acesso à internet, seja desktop, notebook ou até mesmo celulares, todos com preços módicos e acessíveis à sociedade brasileira.

Conforme assevera Gabriel Bonis, os computadores cada vez mais tem ganhado espaço nos lares dos brasileiros, sendo que em 2011, 45% dos domicílios já tinham computador, contra 35% do ano de 2010, ou seja, um crescimento considerável para um curto espaço de um ano. Embora seja um número crescente, está muito abaixo das estatísticas da União Europeia onde a média de pessoas com acesso a internet chega a 73% da população.

Atualmente, em pesquisa realizada pelo Instituto Brasileiro de Geografia e Estatística (IBGE), no mês de outubro de 2013, constatou-se a continuidade do crescimento do percentual de pessoas com acesso à internet, chegando ao total de oitenta e três milhões de pessoas com

---

[10] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1 ed. 2ª tiragem, Saraiva: São Paulo, 2011. p. 32.
[11]IBOPE. Acesso à internet no Brasil atinge 94,2 milhões de pessoas. Disponível em: <http://www.ibope.com.br/pt-br/noticias/paginas/acesso-a-internet-no-brasil-atinge-94-milhoes-de-pessoas.aspx>. Acesso em: 06 mar. 2013.

idade acima de dez anos, as quais declararam ter acesso à internet, o que corresponde a 49,2% dos brasileiros nesta faixa etária. [12]

Ainda, em relação ao Brasil, urge destacar que a maioria da população com acesso a internet é oriunda das regiões Sul, Sudeste e Nordeste, totalizando 87%; e o público que mais acessa a rede mundial tem entre 10 e 34 anos, chegando a um total de 52%[13].

Já no que concerne ao local de acesso à rede, as *Lan Houses* são lugares que possibilitam o maior número de acessos a internet, embora haja grande diminuição deste tipo de locais de acesso. Desde o ano de 2009, verifica-se que continua sendo um dos principais locais utilizados para acesso a internet,[14] o que dificulta inclusive a elucidação de crimes cibernéticos realizados a partir destes pontos de acesso, considerando o número de pessoas que fazem uso destes computadores, bem como que, na maioria das vezes não se tem um controle em relação à data e hora que cada pessoa utilizou a máquina, o que pode ser resolvido com a criação de um cadastro individual para cada cliente, bem como o registro da data e hora que o indivíduo utilizou determinado computador.

Desse modo, pode-se constatar que, além de haver um público definido especialmente pela região, há também uma divisão em relação à idade dos usuários da rede, cuja maioria é estudante ou pessoas que utilizam o computador como ferramenta de trabalho.

O objetivo principal que gira em torno do avanço tecnológico da comunicação sempre foi à criação de uma aldeia global o que consequentemente facilita o contato entre pessoas em diferentes partes do mundo, permitindo assim a troca de informações e realização de negócios, tudo isso com custo reduzido, se comparados aos gastos com telefone, papeis, viagens e etc.[15]

> No mundo da **Infoera**, as informações vão se propagar imediatamente e estarão instantaneamente disponíveis a todos os infocidadãos. Mas, não só as informações: através do uso cada vez mais corrente da moeda eletrônica e do dinheiro virtual, também recursos financeiros poderão ser rapidamente transferidos, sem aparentes barreiras e sem aparentes controles.[16]

---

[12]Exame.com. **Número de brasileiros com acesso à Internet chega a 83 milhões**. Disponível em <http://exame.abril.com.br/tecnologia/noticias/numero-de-brasileiros-com-acesso-a-internet-cresce-7> acesso em 03/11/2013.

[13] BONIS, Gabriel. **Carta Capital, Sociedade, Quase metade dos lares brasileiros já tem computadores**. Disponível em <http://www.cartacapital.com.br/sociedade/quase-metade-dos-lares-brasileiros-tem-computador/> acesso em 06/03/2013 as 15:25.

[14]CETIC.br. **Pesquisa TIC Domicílios 2010**. Disponível em :<http://www.cetic.br/usuarios/tic/2010/apresentacao-tic-domicilios-2010.pdf> Acesso em 19/04/2013.

[15] PINHEIRO, Patrícia Peck, **Direito Digital**. 4 ed. São Paulo, Saraiva. 2010. p. 63.

[16] ZUFFO, João Antonio. **A Sociedade e a Economia no Novo Milênio: Os Empregos e as Empresas no Turbulento Alvorecer do Século XXI.** Livro I – A Tecnologia e a Infosociedade. São Paulo, Manole. 2003. p. 225 e 226.

Assim, como a sociedade se desenvolve e fica mais dinâmica a cada dia, consequentemente ocorre uma mudança cultural, mudança esta que acontece em espaços de tempo cada vez menores e, se as pessoas mudam seus hábitos, o direito não pode ficar para trás, devendo acompanhar a evolução e adaptar-se a nova sociedade, à sociedade da informação.

Com o advento desta nova era, principalmente a partir da década de 1980 os conceitos e terminologias foram se modificando, e expressões básicas utilizadas no cotidiano daqueles que vivem neste meio passaram a integrar, mesmo que de forma tímida às doutrinas e as Leis, como por exemplo, as expressões *hardware* e *software*, endereço de IP e *firewall*.

Assim, gradativamente, a informatização passa a integrar o direito, e o direito a prever normas em relação utilização das tecnologias da comunicação, tipificando os crimes de informática.

1.3 Conceito de Delitos Informáticos

Inicialmente, cabe esclarecer que, apesar de se ter optado pela nomenclatura "Delito informático" para referir-se aos crimes cometidos no meio virtual, na presente pesquisa não far-se-á qualquer diferenciação entre os termos delito e crime. Feito tal esclarecimento, passa-se a conceituação de crime.

Nas lições de Fernando Capez[17], crime pode ser dividido sob três aspectos, sendo eles, material, formal ou analítico. O primeiro aspecto tratado, o material, relaciona-se com a essência do conceito. Visa explicitar o motivo de o fato ser considerado crime, podendo ser definido como fato humano que realizado de forma dolosa ou culposa causa lesão ou expõe a perigo os bens resguardados pela ordem jurídica.

> Aspecto material: é aquele que busca estabelecer a essência do conceito, isto é, o porquê de determinado fato ser considerado criminoso e outro não. Sob esse enfoque, crime pode ser definido como todo fato humano que, propositada ou descuidadamente, lesa ou expõe a perigo bens jurídicos considerados fundamentais para a existência da coletividade e da paz social[18].

[17] CAPEZ, Fernando. **Curso de direito penal**. Volume 1, parte geral: (arts. 1º a 120). 15. ed. — São Paulo: Saraiva, 2011. p.135.
[18] Ibidem. p. 135.

Dessa forma, o aspecto material nada mais é que a conduta humana que, seja por vontade do agente, ou por descuido, cause prejuízo ou exponha a perigo os bens resguardados pelas normas jurídicas, essenciais para existência de uma convivência pacífica em comunidade.

Já o aspecto formal do conceito de crime relaciona-se à norma posta, de modo que, pouco importa o motivo pelo qual o bem foi tutelado, cabendo ao cidadão simplesmente o dever de observar estas normas para que não incorra na prática das condutas ali descritas, sob pena de ser-lhe aplicada uma sanção.

> Aspecto formal**:** o conceito de crime resulta da mera subsunção da conduta ao tipo legal e, portanto, considera-se infração penal tudo aquilo que o legislador descrever como tal, pouco importando o seu conteúdo. Considerar a existência de um crime sem levar em conta sua essência ou lesividade material afronta o princípio constitucional da dignidade humana[19].

Conforme verifica-se da lição de Fernando Capez, o aspecto formal do crime diz respeito às normas elaboradas pelo legislador, não havendo relevância se o fato lesionou ou expôs a perigo os bens jurídicos, ressaltando ainda que considerar determinada conduta como crime, sem sopesar a essência, bem como a lesão que tal conduta possa causar, é ir na contra mão do princípio da dignidade humana, previsto na Constituição Federal.

De outro norte, o aspecto analítico, como o próprio nome sugere, faz uma análise maior do contexto, levando em conta não somente a norma posta ou a lesão ao direito de terceiro, pois não basta o agente cometer o fato descrito como crime, devendo ser observados outros aspectos, veja-se:

> Aspecto analítico**:** é aquele que busca, sob um prisma jurídico, estabelecer os elementos estruturais do crime. A finalidade deste enfoque é propiciar a correta e mais justa decisão sobre a infração penal e seu autor, fazendo com que o julgador ou intérprete desenvolva o seu raciocínio em etapas. Sob esse ângulo, crime é todo fato típico e ilícito. Dessa maneira, em primeiro lugar deve ser observada a tipicidade da conduta. Em caso positivo, e só neste caso, verifica-se se a mesma é ilícita ou não. Sendo o fato típico e ilícito, já surge a infração penal. A partir daí, é só verificar se o autor foi ou não culpado pela sua prática, isto é, se deve ou não sofrer um juízo de reprovação pelo crime que cometeu. Para a existência da infração penal, portanto, é preciso que o fato seja típico e ilícito[20].

Assim, para que ocorra o crime, deve-se inicialmente verificar a tipicidade da conduta, isto é, se há previsão legal da conduta praticada pelo agente no ordenamento jurídico. Em caso positivo, verifica-se a licitude da conduta que caso seja ilícita, já tem-se aí a infração penal,

---

[19] CAPEZ, Fernando. **Curso de direito penal**. Volume 1, parte geral: (arts. 1º a 120). 15. ed. — São Paulo: Saraiva, 2011. p. 135.
[20] Ibidem. p 135.

restando saber se o autor foi ou não culpado pela prática da conduta, de forma que irá ou não sofrer as sanções impostas pela lei.

Importante valer-se da lição do doutrinador Julio Fabbrini Mirabete, o qual ensina que a finalidade do Estado é o bem coletivo, devendo para tanto, manter a ordem, a harmonia e o equilíbrio social.

Cabe ainda ao Estado velar pela paz interna, pela segurança, bem como pela estabilidade coletiva em relação aos conflitos inevitáveis entre os interesses de particulares e o interesse destes e do poder constituído. Para tanto, necessário se faz valorar bens ou interesses, individuais ou coletivos, protegendo-se, assim através da lei penal, aqueles que são mais atingidos quando há transgressão das normas previstas no ordenamento jurídico. Tal proteção concretiza-se através do estabelecimento e aplicação de penas, havendo previsão legal de determinada conduta e consequente punição daquele que nela incorrer.[21]

Assim, tem-se que, crime é a realização de uma conduta previamente tipificada, da qual decorre uma sanção, desde que não seja o caso de aplicação de excludente de antijuridicidade.

Atendo-se aos delitos informáticos, alguns autores, como Miguel Angel Davara Rodrigues, definem os crimes praticados no meio virtual com a efetivação de uma ação, com as características que delimitam o conceito de delito, consumando-se, através de um elemento informático ou vulnerando os direitos de um titular de um elemento informático, aí sendo entendido um *hardwares* ou *software*.[22]

Ricardo M. Mata Y. Matin dispõe que:

> (...) a conceituação do chamado "crime informático", expressão que prefere por sua simplicidade e por, no seu entender, melhor corresponder com o termo inglês *computer crimes*, deve ser toda ação dolosa que provoca um prejuízo a pessoas ou entidades, utilizando-se, para sua consumação, dispositivos habitualmente empregados nas atividades de informática.[23]

Os delitos informáticos diferenciam-se dos demais crimes especialmente no que diz respeito ao meio empregado para a consumação do ato delitivo, qual seja, o uso de computador ou outro dispositivo que permita o acesso à rede.

---

[21] MIRABETE, Julio Fabbrini. **Manual de Direito Penal**. Parte Geral Arts. 1º a 120 do CP Volume 1. 26 ed. rev. e atual. Editora Atlas S.A.: São Paulo. 2010. p. 82.

[22] LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computacional**. 2ª ed. ATLAS S.A: São Paulo – 2011. p. 10 apud RODRÍGUEZ, Miguel Angel Davara. Derecho Informático. España: Editora Aranzadi, 1993.

[23] MARTIN, Ricardo M. Mata Y. Professor Titular de Direito Penal da Universidade de Valladolid. Aspectos comunes em La delincuencia informática. Madrid: Editora Edisofer, 2001. P. 21-25 apud.LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computacional**. 2ª ed. ATLAS S.A: São Paulo – 2011. p. 10

Ademais, com a popularização da internet e dos computadores, facilitou-se o acesso da tecnologia a todos os públicos, inclusive de pessoas mal intencionadas, pelo que, houve a adaptação nos meios de cometer crimes já tipificados, bem como o surgimento de novos crimes, que embora trouxessem prejuízo a outrem, não havia tipificação na lei para punir o autor do fato, conforme ensina Marcelo Xavier de Freitas Crespo.

> (...) se até a terminologia se alterou, não haveria de ser diferente com a criminalidade. Esta também encontrou novas formas se de fazer presente, até porque, em alguns casos, há lacunas da lei penal e, como não pode haver analogia *in malam partem*, há condutas certamente prejudiciais, mas que não são ainda tipificadas como delito. Além disso, se os bens jurídicos afetados com a criminalidade não informática eram os individuais, com a sociedade digital globalizada, outros bens jurídicos passaram a ser afetados (bens difusos).[24]

Em outras palavras, o avanço tecnológico reduz o planeta transformando-o em uma aldeia, possibilitando a comunicação com qualquer pessoa, pouco importando a distância. A efetivação deste conceito se dá com um mundo globalizado e o estreitamento das relações, políticas, econômicas e sociais, tudo isso, resultado da evolução da tecnologia da informação e comunicação, especialmente da *World Wide Web.*[25] Todos esses avanços viabilizam o cometimento de ilícitos que causam lesão à coletividade, trazendo prejuízos a bens comuns do povo.

Inúmeros são os benefícios trazidos como o advento da era da informação. Contudo, todavia, esses pontos positivos vêm acompanhados de malefícios, os crimes e criminosos virtuais, que aumentam de forma alarmante em todo o mundo, criando assim um risco potencial se levado em conta os prejuízos econômicos, a privacidade, bem como outros bens jurídicos tutelados, que ainda serão objeto da tutela estatal. Os computadores adentraram de tal forma em nosso cotidiano que se torna a cada dia mais irreversível nossa dependência às máquinas[26].

Em síntese, conforme a doutrina, dentre elas a de Marcelo Xavier de Freitas Crespo, há duas categorias de crimes digitais, sendo eles os próprios e os impróprios. Para o cometimento dos crimes relacionados a esta segunda categoria, não se faz necessário grande conhecimento técnico, eis que embora o meio seja diferente, o ambiente virtual foi apenas um novo local encontrado para praticar delitos já descritos como crime.

Por outro lado, os ilícitos classificados como próprios, dependem de um conhecimento técnico específico para a computação, são os crimes praticados por pessoas que detêm um maior

---

[24]CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1 ed. 2ª tiragem, Saraiva: São Paulo. 2011. p. 36/37.
[25] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1 ed. 2ª tiragem, Saraiva: São Paulo. 2011. p. 36.
[26] LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computacional**. 2ª ed. ATLAS S.A: São Paulo – 2011. p. 6.

conhecimento na área da Tecnologia da Informação[27]. A diferenciação entre os delitos informáticos próprios e impróprios será retomada no decorrer da pesquisa.

Um dos maiores problemas em relação aos crimes cibernéticos é que em grande parte das vezes o criminoso não pode ser visto ou ouvido, ou seja, não há testemunhas e, ainda, pode atingir várias pessoas ao mesmo tempo e de qualquer local do mundo, bastando para tanto estar conectado na internet, tudo isso sem sair do conforto do seu lar.

Porém, a culpa da ocorrência de crimes na rede não deve recair sob os equipamentos eletrônicos, pois estes são simplesmente o meio utilizado pelo autor do delito.

Nesse sentindo, assevera Paulo Marco Ferreira Lima,

> Em verdade, os crimes de computador são, na maior parte das vezes, os crimes comuns cometidos com auxílio de um computador, podendo os crimes de furto, apropriação indébita, estelionato ou dano, serem cometidos por esse meio com consideráveis prejuízos patrimoniais. Entretanto, há algo além de uma nova ferramenta, de um novo meio, de um novo *modus operand* para cometimento de crimes: estamos também diante de novas condutas não tipificadas[28].

Para que possa desempenhar seu papel fielmente, cumprindo a finalidade para qual foi criado, o direito deve sempre acompanhar a evolução da sociedade, de forma que não haja injustiças. Considerando as constantes mudanças culturais, bem como a forma como se altera o modo de pensar das pessoas, neste ambiente cultural onde as mudanças ocorrem com espaços de tempo cada vez menores, cabe ao legislador criar normas que estejam de acordo com as novas necessidades da sociedade,

Relevante neste ponto, demonstrar a distinção entre Informática Jurídica e Direito da Informática, que embora, a primeira vista pareçam termos similares ou idênticos, são muito distintos, conforme explica Marcelo Xavier de Freitas Crespo:

> A Doutrina define a Informática Jurídica como o ramo da Informática que compreende as suas aplicações específicas ao mundo do Direito, complementando o trabalho daqueles que operam com o Direito através do processamento e armazenamento eletrônico das informações jurídicas. Em outras palavras, trata-se do estudo da aplicação da informática como instrumento, e o consequente impacto na produtividade dos profissionais do Direito. Já o Direito da Informática é definido como o ramo do Direito que delineia, estuda e busca resolver os problemas jurídicos advindos da evolução tecnológica[29].

Ante a explicação supra, torna-se fácil a compreensão da diferença entre Direito da Informática e Informática Jurídica, sendo que o primeiro é o ramo do direito que estuda e busca

---

[27] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1 ed. 2ª tiragem, Saraiva: São Paulo. 2011. p. 94.
[28] LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computacional**. 2ª ed. ATLAS S.A: São Paulo – 2011. p. 11.
[29] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1 ed. 2ª tiragem, Saraiva: São Paulo. 2011. p. 38.

resolver os problemas advindos da evolução da informática, os novos impasses, ou problemas já existentes que passaram a ocorrer de novas formas com o advento da era da informação.

De outro lado, informática jurídica trata-se da inserção da tecnologia da informação no meio jurídico, ou seja, a forma pela qual o direito se moderniza e acompanha o desenvolvimento da sociedade, como a velocidade na troca de informações, economia de materiais como papeis tintas de impressoras e locais de armazenamento.

Os delitos informáticos podem ainda ser definidos como as condutas de acesso não autorizado a sistemas digitais, ações que tragam prejuízos a esses sistemas, a interceptação de comunicações, as modificações de dados, a pornografia infantil, o dano informático, a espionagem eletrônica, os crimes contra a propriedade intelectual, os crimes contra à honra, a invasão de privacidade, estelionato e as fraudes virtuais[30].

Vários são os tipos de crimes relacionados aos meios virtuais e por se tratar de um tema relativamente novo, ainda não há termos especificamente definidos para as ações criminosas cometidas na rede, eis que vários são os termos adotados pelos diferentes autores.

Os termos utilizados para definir crimes praticados em ambiente virtual são vários, sendo que não há um consenso acerca de qual é a melhor denominação para os delitos praticados na rede, dentre eles pode-se verificar os crimes de computação, delitos de informática, abuso de computador, fraude informática, ou seja, os conceitos ainda não englobam todos os crimes ligados à tecnologia e, portanto, deve-se tomar cuidado ao conceituar determinados crimes, tendo em vista que existem muitas situações complexas no ambiente dos crimes ocorridos na rede[31].

Outrossim, embora existam várias denominações para conceituar os crimes praticados nos meios eletrônicos, grande parte da doutrina optou pelo termo "Crimes Digitais".

Importante frisar que embora existam vários termos para definir os crimes praticados no meio virtual, os quais se alteram ao longo do tempo para abranger os novos tipos de crime, bem como as formas de cometê-los, na presente pesquisa, adota-se o termo delitos de informática, por ser esta a nomenclatura utilizada pela legislação pátria, em especial pela Lei 12.737/2012.[32]

Em relação à prática dos primeiros delitos informáticos, a presença de pessoas de má-fé no meio virtual é tão antiga quanto o surgimento dos primeiros equipamentos de informática, momento que já se tem notícia dos primeiros atos lesivos praticados através de computadores.

---

[30] PINHEIRO, Patrícia Peck, **Direito Digital**. 4 ed. São Paulo, Saraiva. 2010. p. 46.
[31] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1 ed. 2ª tiragem, Saraiva. 2011: São Paulo. p. 58.
[32] Lei 12.737/2012. 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.

Há que se ressaltar os inúmeros benefícios advindos da era da informação, todavia, estes vieram acompanhados de pontos negativos, sendo um deles a má-fé de usuários que utilizam da tecnologia para cometimento de crimes, crimes estes que em inicialmente objetivavam apenas a demonstração de conhecimento dos programadores, ou seja não causavam prejuízos às vítimas, no máximo algum transtorno. Com a popularização da internet e das transações virtuais, logo atraiu a atenção de pessoas mal intencionadas e, consequentemente, surgiram os primeiros delitos informáticos.

Assim como nos demais crimes, no mundo virtual, para a existência do ato delitivo é necessário a existência de um agente ativo (autor) e um agente passivo (vítima). O referida temática abordar-se-á em seguida.

1.4 – Sujeitos do Delito Informático

Assim como nos demais crimes, nos delitos de informática existe o sujeito ativo, que é o criminoso, aquele que incorre na conduta descrita na norma penal e, de outro lado, a vítima, que é aquela que tem seu bem jurídico tutelado ferido, isto é, que experimenta algum prejuízo em consequência da conduta do criminoso.

Todavia, nos delitos informáticos, necessário se faz que os sujeitos, vítima e criminoso, utilizem qualquer dispositivo informático, uma vez que este é o meio para o cometimento do crime.

1.4.1 - Sujeito Passivo

Pode-se definir sujeito passivo ou vítima dos crimes de computador, como o ente sobre o qual recai a conduta omissiva ou comissiva praticada pelo sujeito ativo, podendo, no caso dos crimes cibernéticos, as vítimas serem indivíduos, instituições creditícias, ou mesmo governos, com tanto que façam uso dos sistemas de informação, estando estes ou não conectados à internet.[33]

[33] LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computacional**. 2ª ed. ATLAS S.A: São Paulo – 2011. p. 36.

Grande parte das vezes, os crimes cibernéticos ocorrem por ingenuidade, bem como falta de conhecimento das vítimas que recebem e-mails desconhecidos e acessam links que não sabem a procedência, ou fornecem informações pessoais para pessoas que se passam por instituições financeiras ou mesmo órgãos do governo.

Ainda, dificilmente se chegará a um número exato no que diz respeito às vítimas dos delitos informáticos próprios, ou seja, aqueles no qual se exige uma maior capacidade de conhecimento técnico do agente que comete a ilicitude.

Tal fato justifica-se pelo motivo de grandes empresas, como bancos não comunicarem à polícia, ou não tomarem as medidas judiciais cabíveis, a fim de não promoverem publicidade negativa. Todavia, entende-se que estas instituições financeiras (devido às falhas de segurança digital em seus serviços *on line*), são as principais vítimas destes crimes[34].

Logo, o ente afetado pelo crime digital, isto é, a vítima, pode ser qualquer pessoa, física ou jurídica, inclusive de natureza pública ou privada.

1.4.2 - Sujeito Ativo

Para a grande maioria das pessoas, quando se fala em sujeito ativo de delitos informáticos, a primeira palavra que vem a cabeça é "*hacker"*, como sendo estes os grandes vilões da informática. Todavia, há uma gama denominações relativas aos autores destas condutas ilícitas.

Dentre as várias nomenclaturas existentes para referir-se aos criminosos virtuais, Marcelo Xavier de Freitas Crespo[35] nos apresenta as seguintes:

Hackers, que é um nome genérico, define os chamados "piratas" de computador, sendo que a melhor tradução para a palavra da língua inglesa é *fuçador*;

Crackers, considerados os verdadeiros criminosos da rede, ocupam-se de invadir e destruir sites, nesta categoria estão presentes também ladrões, valendo-se da internet para subtrair dinheiro e informações, sendo o termo *Cracker*, a expressão consagrada para denominar os criminosos que utilizam os computadores como armas;

---

[34] Ibidem. p. 37.
[35] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1 ed. 2ª tiragem, Saraiva: 2011: São Paulo. p. 95/98.

Carders, neste grupo estão compreendidos os estelionatários virtuais, têm essa nomenclatura em razão de utilizarem cartões de créditos alheios ou gerados através de programas de computadores;

Lammers, pessoas que se autointitulam *hacker*, todavia, não dispões de todo conhecimento quanto dizem e geralmente são insultados e depreciados pelos *hackers*;

Wannabes, pode-se considerar que estão entre os *hackers* e os *lammers*, isto é, não possuem todo o conhecimento necessário para praticar grandes atos na rede, porém já tem capacidade de demonstrar aquilo que sabem, podendo inclusive causarem prejuízos a outrem;

Phreakers, pode-se classificá-los como hackers da telefonia, ou seja utilizam de seu conhecimento para realizar escutas telefônicas, bem como ligações gratuitas.

White e Black hats, termo utilizado para definir os "bons" e "maus" *hackers*, em uma tradução livre seria "chapéu branco" e "chapéu preto", respectivamente os bons e os maus.

Interessante esclarecer que o termo "hacker" é erroneamente utilizado para referir-se aos criminosos da rede. Tal adjetivo trata-se de um equívoco, uma vez que tal nomenclatura, em sua origem fazia referência às pessoas que dominavam o conhecimento, inicialmente na eletrônica e posteriormente na informática e eram capazes de fazer modificações inteligentes nos hardwares e softwares, no mesmo sentido é a lição e Edson Pedroso.

> A palavra "hack" nasceu num grupo chamado Tech Model RailRoad Club (TMRC) na década de 50. Membros do clube (soldier e ChAoS) chamavam as modificações inteligentes que faziam nos relês eletrônicos de 'hacks'. Quando as máquinas TX-0 e PDP-1 chegaram ao mercado os membros do TMRC começaram a utilizar o mesmo jargão para descrever o que eles estavam fazendo com a programação de computadores. Isso continuou por anos até mesmo quando novas máquinas como o PDP-6 e depois o PDP-10 apareceram. O termo passou a ser usado com diversos significados: sucessos em determinadas áreas, fosse como uma solução não óbvia e particularmente elegante para um problema, ou uma partida inteligente pregada a alguém, ou ligar os sistemas informáticos e telefônicos para fazer chamadas grátis. Eventualmente, o termo passou a ser utilizado exclusivamente nas áreas da programação ou eletrônica, em que passou a ser usado para designar indivíduos que demonstravam capacidades excepcionais nestes campos, efetivamente expandindo-os com atividades práticas e artísticas.[36]

Assim, o termo *hacker* não é corretamente empregado pela sociedade de uma forma geral, vez que utilizam tal nomenclatura para referir-se a todos que tem conhecimento técnico elevado em relação à tecnologia da informação, pouco importando se atuam prevenindo e repelindo ameaças virtuais ou se são causadores de tais ameaças.

---

[36]PEDROSO, Edson, **Termo Hacker, qual seu significado**?. Disponível em <http://www.oficinadanet.com.br/artigo/1476/termo_hacker_qual_seu_significado>. Acesso em 17 de abril de 2013.

Ademais, conclui-se que a causa de tal termo ser difundido de maneira errônea, isto é, sem diferenciar que *hacker* é o termo empregado a aquele que utiliza seu conhecimento digital de forma correta, sem ultrapassar os limites da Lei, enquanto que *crackers* e as demais definições de criminosos virtuais, raramente são empregadas, principalmente pela falta de conhecimento de quem transmite os acontecimentos relacionados aos crimes, ou grandes feitos da era da informação.

1.5 – Surgimento dos Delitos informáticos

As primeiras notícias de crimes cibernéticos datam da década de setenta[37], geralmente eram praticados por pessoas com conhecimentos avançados na área de informática, visando burlar a segurança de empresas, especialmente de instituições financeiras, como bancos. Hoje em dia modificou-se bastante o perfil dos criminosos virtuais, eis que os usuários da internet mudaram. Atualmente, qualquer pessoa, inclusive as que não detem conhecimento técnico avançado, mas que possuem acesso à internet podem praticar crimes pelo meio virtual, até mesmo o usuário doméstico possui conhecimento maior acerca do uso de computadores e tecnologias voltadas para internet.

Uma das primeiras ameaças de computador foi criada no ano de 1971, em um laboratório, denominado de *Creeper Virus*, foi desenvolvida por um funcionário chamado Bob Thomas, da empresa que trabalhava com a construção da ARPANET, era um vírus autorreplicante, tratava-se de um artefato malicioso.[38]

Já no ano de 1984, Fred Cohem apresentou um trabalho denominado *Experiments with Computer Viruses*, momento em que foi criado o termo "vírus de computador" o qual denomina programas maliciosos, prejudiciais ao sistema como um todo[39].

O primeiro antivírus que se tem notícia foi criado no ano de 1988 por Denny Yanuar Ramdhani, na Indonésia e seu objetivo era imunizar o sistema operacional contra o vírus Brain, o primeiro vírus a causar transtornos e que se espalhou por todo o mundo[40].

---

[37] PINHEIRO, Patrícia Peck, **Direito Digital**. 4 ed. São Paulo, Saraiva. 2010. p. 44 e 45.
[38] WENTED, Emerson. JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport, 2012. p. 10.
[39] WENTED, Emerson. JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport, 2012. p 10.
[40] Op. Cit. p. 11.

Nesse contexto, verifica-se que a presença de pessoas de má-fé no mundo da informática é verificada desde o surgimento da mesma, bem como que os criminosos evoluem junto com a tecnologia, sempre criando formas alternativas de cometerem seus atos danosos. Ainda, importante ressaltar a dificuldade que o Estado encontra para reprimir os agentes que cometem delitos informáticos, uma vez que a tecnologia avança em velocidade imensurável, o que é acompanhado pelos criminosos da rede, enquanto que, para a criação de Leis que possam punir os infratores, necessário se faz um processo lento e cheio de burocracias, o que, dificulta para o legislador a aplicação das normas, devendo fazer uso de analogia, quando não houver previsão legal.

1.6 - O problema da persecução criminal nos delitos informáticos

Não é uma tarefa fácil analisar as condutas praticadas através do meio cibernético, até porque o agente pode praticar o crime de vários lugares, uma vez que os crimes digitais não encontram barreiras. Para o criminoso cometer a atitude ilegal, basta ter acesso à rede.

Grande parte dos crimes cometidos por meios digitais são verificados também no "mundo real". Nesse contexto, a internet surge apenas como um facilitador, principalmente devido ao fato da dificuldade de encontrar aquele que cometeu o ato delituoso. De outro lado, é também uma barreira para a persecução criminal, pois, é necessário profissionais capacitados para realizarem a investigação neste tipo de delito, tendo em vista a necessidade de conhecimento técnico informático.

Os conceitos de crime, delito, ato e efeito são os mesmos aplicados tanto no âmbito do direito penal como do direito penal digital, cibernético ou eletrônico, sendo que as principais diferenças referem-se à territorialidade e à investigação de provas, bem como a criação de novos tipos penais em virtude do surgimento de crimes que são cometidos exclusivamente através dos meios eletrônicos.[41]

A persecução penal de forma geral pode ser dividida em duas fases, quais sejam: Investigação Criminal e Processo Penal. Enquanto a primeiro atem-se a colheita de provas, à apuração de indícios de autoria e materialidade da ação delitiva, a segunda fase tem por escopo processar e julgar.

---

[41] PINHEIRO, Patrícia Peck, **Direito Digital**. 4 ed. São Paulo, Saraiva. 2010. p. 296 e 297.

Jorge Higor Vinicius Nogueira e Emerson Wendt na obra Crimes Cibernéticos, Ameaças e procedimentos de investigação, dividem a fase investigatória em duas, sendo elas fase técnica e fase de campo.

Na fase técnica, o objetivo principal é localizar o computador utilizado para realizar a ação criminosa, procedendo-se as seguintes atitudes: análise dos relatos da vítima, a fim de compreender o fato ocorrido; instruir a vítima para que haja de forma a preservar o material a ser utilizado como prova; coleta das primeiras provas no ambiente virtual; formalizar o registro da ocorrência do fato criminoso, através da confecção de um boletim de ocorrência; maiores investigações acerca do fato, das informações disponíveis na rede, prováveis autores, origens de e-mails, hospedagem de domínios; confecção de relatório ou certidão referente as provas coletadas e apurações preliminares; solicitação de autorização, junto ao poder judiciário, para quebra de sigilo de dados, conexão ou acesso e; por fim, a análise das informações prestadas pelos provedores de conexão ou conteúdo.[42]

As referidas medidas, destarte, são as primeiras a serem tomadas na fase inquisitorial, para assegurar o correto deslinde do processo na fase judicial, propiciando ao juiz todos os elementos necessários para julgar o feito.

Fundamental para o deslinde na fase processual é a realização de uma boa investigação na fase inquisitiva, de forma que sejam cumpridos os passos necessário para apuração do delito, realizando as formalidades necessárias, desde a coleta inicial de provas, a fim de resguardar o material probatório passível de ser perdido, após, formalizando a ocorrência do delito e seguindo a linha de investigação, apurando, através das formas admitidas em lei a autoria e a materialidade do delito.

Caso necessário para as investigações, após autorização judicial, poderá realizar-se a quebra do sigilo de dados telemáticos (Logs, IP's), bem como solicitados dados cadastrais, constantes de provedores, de forma a complementar o conjunto probatório.

Ainda, importante resaltar que sempre que um computador, ou dispositivo similar (celular, tablet etc.) conecta-se a internet, um endereço de IP (Internet Protocol) é atribuído exclusivamente a aquele equipamento, ou seja, não existem dois IP's iguais sendo utilizados simultaneamente.[43]

---

[42] WENTED, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport, 2012. p. 52 e 53.

[43] WENTED, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport, 2012. p. 53.

Superada essa fase, isto é, após ser localizado o computador que permitiu o acesso criminoso, tem-se início a fase campo, na qual se faz necessário o deslocamento dos agentes policiais para procederem ao reconhecimento do local onde se encontra o equipamento por meio do qual se realizou o ato delitivo.

Tal diligência deverá ser feita de maneira sutil, uma vez que poderá ser necessário solicitar uma medida cautelar, para assegurar a produção de provas, para o que deve haver a representação para que o poder judiciário conceda o mandado de busca e apreensão do equipamento eletrônico. O que ocorrerá logo que se identificar o endereço que corresponda a uma residência ou rede não corporativa.[44]

Dentre os elementos investigados nos delitos informáticos, tem-se o *log*[45] gerado pela conexão à internet ou outro serviço da rede mundial pelos provedores de conteúdo ou e-mail.

Com as informações descritas pelo *log*, poderá ser identificado o computador que o indivíduo utilizou para realizar a ação delitiva. Todavia, pode tratar-se de um computador de uso coletivo, como em uma *lan house* ou uma rede corporativa, caso em que, pela via judicial será solicitado que o responsável pelo equipamento de onde originou o acesso criminoso informe os dados relativos ao computador e ao indivíduo a quem foi atribuído o IP, levando-se em conta o dia e horário do acesso.[46]

1.6.1 Do Lugar do Crime – Ciberespaço

Tendo em vista a possibilidade de acessar outro equipamento em qualquer local do mundo a partir de um dispositivo conectado à internet, torna-se fácil cometer crimes, mesmo estando distante do local do resultado, uma vez que através da internet é possível cometer crime, ainda que este esteja em outro continente.

Surge então o problema da aplicação da norma penal no espaço, eis que, levando em consideração as características dos delitos informáticos acima elencados, é possível que um

---

[44] Ibidem. 54.

[45] WENTED, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport, 2012. O *log* de conexão é um conjunto de informações sobre a utilização de internet pelo usuário, contendo data, horário, fuso horário, duração da conexão e número de protocolo de internet, mais conhecido como IP (*Internet Protocol*). Já o *log* de acesso é um conjunto de informações sobre a utilização de determinado serviço na internet (relativos aos provedores de conteúdo) pelo usuário, contendo data, horário e número do IP. p. 177.

[46] WENTED, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport, 2012. p. 177.

criminoso no Brasil, invada uma determinada conta bancária no Japão e transfira dinheiro para uma conta na Suíça. Diante desta problemática surge o questionamento em relação á competência jurisdicional do juízo penal.Conforme Marcelo Xavier de Freitas Crespo:

> Assim, os crimes digitais podem ser praticados parcialmente em diversos países, fragmentando-se o *iter criminis*. Questões sobre a presença física para a prática delitiva, bem como fronteiras territoriais ganham novas perspectivas, de modo que algumas características se mostram frequentes: a velocidade com a qual o delito é praticado, a distância a partir da qual se cometem os crimes, o volume de dados envolvido. Consequentemente, questões relativas à prova processual também ganham destaque[47].

Em nosso ordenamento jurídico, embora tenham surgidos novas normas com o escopo de legislar acerca da matéria dos delitos informáticos, ainda encontra-se muito carente de legislação específica ao tema, principalmente no que diz respeito aos tratados internacionais. Dessa forma devem os países se dedicarem no combate destes crimes, tendo vista a dificuldade da questão da produção de provas e do local onde o agente que cometeu o crime será processado e julgado.

> Neste contexto, surgem dúvidas em relação ao local da aplicação da norma penal, tendo em vista que a conduta criminosa foi cometida em um local e o resultado se deu em outro, possivelmente com legislação diferente. Conforme Marcelo Xavier de Freitas Crespo:É de se considerar que, nesse sentido, ganham destaque as questões sobre qual a teoria aplicada para definir o local do crime. Vêm a lume as teorias da atividade, do resultado e da ubiquidade. Pela primeira, o lugar do crime é o da ação ou da omissão, ainda que outro fosse o do resultado. Pela segunda, despreza-se a conduta, privilegiando-se o lugar onde se deu o resultado. Por seu turno, a teoria da ubiquidade conjuga as duas outras, entendendo o crime praticado tanto no lugar da conduta como no lugar em que se produziu o resultado.[48]

O legislador pátrio adotou a teoria da ubiquidade, conforme dispões o art. 6º[49] do Código Penal, fato que, teoricamente soluciona os problemas relativos ao Direito Penal Internacional, possibilitando que sejam aplicadas as leis brasileiras a crimes cometidos fora do nosso território legal, conforme determina o art. 7º do mesmo diploma legal.

Conforme ensina Patricia Peck Pinheiro, deve-se tomar como base o direito internacional, o qual estabeleceu que, diante da extrapolação dos limites territoriais é este quem identifica a norma a ser aplicada, ou seja deve-se verificar o país onde o agente cometeu a conduta criminosa, bem como aquele onde surtiram os efeitos do ato.[50]Patrícia Peck Pinheiro assevera que,

---

[47] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1 ed. 2ª tiragem, Saraiva. 2011: São Paulo. p. 117.
[48] Ibidem. p. 118.
[49] Art. 6º Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado.
[50] PINHEIRO, Patrícia Peck, **Direito Digital**. 4 ed. Saraiva: São Paulo, 2010. p. 80.

> Aqui entra um dilema importante, que não se aplica no mundo real: na Internet, muitas vezes não é possível reconhecer facilmente de onde o interlocutor está interagindo. Muitos *sites* têm terminação ".com", sem o sufixo de país (por exemplo o ".br" em seguida) o que teoricamente significa que estão registrados nos Estados Unidos. Só que vários deles apenas estão registrados nos Estados Unidos e não têm nenhuma existência física nesse país. Uma tendência mundial é assumir definitivamente o endereço eletrônico como localização da origem ou efeito do ato. Assim, se uma empresa brasileira registra um *site* como ".com", em vez de ".com.br", pode ter de se sujeitar às leis de diversos países no caso de questões jurídicas.[51]

Assim, pode-se constatar que a terminação do endereço do site, adquire relevância, tendo em vista que, além de identificar a origem do site, isto é, a qual país pertence, é fator que determina a legislação a ser aplicada, em caso de delitos informáticos internacionais.

Segue a citada autora, lecionando acerca dos princípios concernentes a aplicabilidade das normas em relação à territorialidade e, aduz que, entre os princípios existentes destacam-se: o princípio do endereço eletrônico, o princípio do local onde a conduta se realizou ou exerceu seus efeitos, o do domicílio do consumidor, o da localidade do réu e o da eficácia na execução judicial.[52]

Em nosso ordenamento tem-se, conforme já mencionado, os artigos 6º e 7º, e ainda o 5º, todos do Código Penal, os quais possibilitam o alcance da grande maioria dos crimes cibernéticos que envolvam brasileiros, mesmo que cometidos a nível internacional.

Todavia outro grande problema enfrentado é a falta de legislação específica para cada conduta criminosa praticada no âmbito dos delitos informáticos, o que deixa muitos criminosos sem puniç ão. No entanto espera-se uma melhora na aplicação de sanções para estes maus elementos da sociedade virtual, com o surgimento de novas leis referente ao tema, como é o caso da Lei 12.737 de 2012.

1.6.2 - Falta de legislação específica

Outro fator que contribui para a impunidade de condutas criminosas na rede é a falta de legislação específica para os delitos informáticos, o que na maioria das vezes obriga o legislador a recorrer ao Código Penal e aplicar os crimes já tipificados, embora não haja menção ao meio eletrônico para seu cometimento. Para Maria Neves,

> Na ausência de uma lei específica, a Justiça tem recorrido principalmente ao Código Penal (Decreto-Lei 2.848/40) para punir os chamados crimes digitais ou cibernéticos.

[51] Ibidem p. 81.
[52] Ibidem. p. 82.

> O relator do projeto que tipifica essas condutas (PL 84/99), deputado Regis de Oliveira (PSC-SP), estima que cerca de 95% dos crimes praticados na rede mundial podem ser julgados com base na legislação vigente. No entanto, para os 5% restantes pode imperar a impunidade[53].

Dos crimes apontados pelo deputado no texto acima, aqueles que podem ser julgados com base no código penal são os delitos informáticos impróprios, ou seja, aqueles que utilizam a tecnologia apenas como um novo meio de cometer crimes que já eram praticados de outra forma.

> (...) sem lei específica, os crimes típicos de internet dificilmente são punidos, porque a legislação penal não admite analogia. "Se o fato não está definido como crime não há punição; acesso não autorizado a sistema, como aconteceu recentemente na Receita Federal, não é crime, mas passará a ser se o projeto for aprovado."[54]

O projeto de lei acima referido resultou na Lei 12.737, atualmente em vigor no Brasil. Registre-se que o Projeto de Lei nº 84 de 1.999 foi transformado na Lei Ordinária 12.735/2012, realizando alterações no Código Penal, Código Penal Militar e a Lei 7.716, de 5 de janeiro de 1989, tipificando condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares. Vale ressaltar que tal dispositivo teve seus artigos 2º e 3º vetados.[55]

Outra Lei de relevante importância que trata dos cibercrimes é a nº 12.737 de 2012, que alterou o Código Penal, Lei esta que foi denominada "Lei Carolina Dieckmann", devido ao fato de a atriz ter sido vítima de uma das espécies de "cibercrimes", ocasião em que teve sua caixa de e-mail violada e fotos íntimas suas publicadas na internet.[56]

O dever do direito é acompanhar a evolução da sociedade, todavia, sabe-se da dificuldade e os trâmites envolvidos desde a criação de um projeto de Lei até a sanção do mesmo o que gera uma demora demasiadamente prolongada e, unindo isto ao fato que as inovações tecnológicas avançam cada vez mais rapidamente, especialmente no ramo da informática, o que tem-se é o direito sempre um passo atrás da sociedade.

---

[53] NEVES, Maria**. Falta de lei sobre crimes digitais leva à impunidade, diz especialista**. Agência Câmara de Notícias. Disponível em <http://www2.camara.leg.br/camaranoticias/noticias/CIENCIA-E-TECNOLOGIA/192143-FALTA-DE-LEI-SOBRE-CRIMES-DIGITAIS-LEVA-A-IMPUNIDADE,-DIZ-ESPECIALISTA.html> acesso em 18/04/2013

[54] PINHEIRO, Patrícia Peck, **Direito Digital**. 4 ed. Saraiva: São Paulo, 2010. p. 81.

[55] PRESIDÊNCIA DA REPÚBLICA, Casa Civil, Subchefia para Assuntos Jurídicos. Lei nº 12.735, de 30 de novembro de 2012. Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm> Acesso em 18/04/2013.

[56] LEI 'CAROLINA DIECKMANN', que pune invasão de PCs, entra em vigor, G1, Tecnologia e Games. Disponível em <http://g1.globo.com/tecnologia/noticia/2013/04/lei-carolina-dieckmann-que-pune-invasao-de-pcs-passa-valer-amanha.html> Acesso em 18/04/2013.

Com fundamento no princípio da legalidade, esculpido no art. 5º, inciso XXXIX da Constituição Federal de 1988[57], princípio este fundamental no direito penal que assevera que *nullum crimen, nulla poena sine lege*, ou seja, não há crime sem lei anterior que assim o defina, nem pena sem prévia cominação legal.

Devido ao fato de não haver punição sem que haja previsão legal do ato delitivo, isto, aliado a velocidade com que a tecnologia inova-se e o consequente aumento do rol de crimes e as formas de cometê-los, resultando na prática de ações delituosas sem punição, sempre que não houver previsão legal.

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

CAPÍTULO II. CRIMES PRATICADOS POR MEIO DE COMPUTADOR E INTERNET

Doravante será apresentado, o rol dos principais delitos informáticos, com a finalidade de introduzir a temática que baliza a presente pesquisa e será abordada no próximo capítulo, qual seja – a problemática da persecução criminal dos delitos informáticos.

Considerando que os crimes digitais estão inclusos em uma matéria relativamente nova, principalmente no ordenamento jurídico brasileiro, ainda, ciente da diferenciação entre os delitos informáticos próprios e impróprios, buscar-se-á demonstrar brevemente o rol dos principais crimes relativos ao meio virtual de acordo com sua categoria já anteriormente analisadas, dividindo-os em próprios e impróprios.

2.1- Dos crimes de informática e suas categorias

Antes de discorrer acerca de cada um dos delitos informáticos aqui elencados, é preciso explicitar a dicotomia existente entre as duas categorias em que estes se dividem, ou seja, a diferença entre os delitos cujo bem tutelado refere-se aos bens eletrônicos, e aqueles onde o meio eletrônico é o instrumento utilizado para lesar outro bem.

Conforme a doutrina de Marcelo Xavier de Freitas Crespo, os delitos informáticos próprios podem também ser chamados de delito de risco informático, enquanto delitos informáticos impróprios são denominados delitos vinculados à informática, veja-se "As condutas praticadas contra um sistema informático telecomunicações ou dados são o que se pode chamar de delito de risco informático, ao passo que as demais podem ser denominadas delitos vinculados á informática."[58]

Dessa forma, os delitos de risco informático referem-se àqueles que têm como objeto um sistema informático ou de dados, de forma que não existiriam, caso não houvesse o meio eletrônico para serem realizados. Ou seja, são tipos penais criados exclusivamente para tutelar os crimes praticados no ambiente virtual.

[58] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1 ed. 2ª tiragem, Saraiva: 2011: São Paulo. p. 63.

Urge ainda, destacar que o agente ativo dos crimes de informática propriamente dito, crimes esses cujo bem tutelado são os sistemas informatizados ou telecomunicações de dados, são pessoas de grande conhecimento técnico, dentre eles os *crackers*, *carders*.

De outro norte, os crimes cuja prática independe da existência de computadores e outras tecnologias similares, condutas ilícitas que podem ser cometidas sem utilizar o meio virtual, considera-se apenas delitos vinculados à informática. Nesse caso, o dispositivo informático é apenas o meio escolhido pelo agente, para praticar conduta que pode ser realizada sem uso de computadores.

Os equipamentos eletrônicos são apenas o meio utilizado para atingir outro bem que não aquele relacionado ao sistema informático ou de dados. Ressalta-se que tal tipo de crime pode ser praticado por qualquer usuário da rede, mesmo aqueles que não detêm conhecimento técnico de informática.

Dessa forma, os delitos informáticos impróprios, são aqueles cuja pratica independem do uso de meio informático. Todavia, o agente optou por valer-se do uso da tecnologia, para a consumação da prática delitiva.

2.2 – Delitos Informáticos Próprios

Ante a diferenciação supra, discorre-se acerca dos crimes cibernéticos próprios, ou seja, aqueles em que os bens jurídicos atingidos são principalmente, sistemas informatizados, telecomunicações ou dados.

2.2.1 – Invasão de Dispositivo Informático

Popularmente conhecido como “invasão”, o acesso não autorizado de dispositivo informático pode se dar por vários motivos, conforme se verifica da lição de Marcelo Xavier de Freitas Crespo:

> A conduta de acessar de forma indevida um sistema informático pode se dar por várias razões, como pelo mero gosto por superar desafios técnicos de segurança, pela vontade de invadir a privacidade alheia tendo acesso a informações sigilosas, ou,

> ainda, por se ter a intenção de manipular, defraudar, sabotar dados. O acesso não autorizado é, portanto, o ilícito básico para a prática de outros tantos possíveis.[59]

Desse modo, entende-se que o acesso não autorizado, conforme o esclarece a própria denominação dada, refere-se ao ato de invadir, ou acessar sistema informático alheio através do uso de equipamento eletrônico.

Em que pese não existir dolo do agente, a simples invasão configura crime, mesmo que o invasor não altere qualquer dado, copie ou destrua arquivos, o simples fato de invadir, já é tido como uma ação criminosa.

Importante salientar que a incriminação da invasão de dispositivo informático é recente em nosso ordenamento jurídico, eis que até bem pouco tempo não havia dispositivo legal que versasse acerca do acesso não autorizado, motivo pelo qual o agente era enquadrado em outras condutas típicas, como, extorsão, estelionato e etc.

Porém, recentemente, mais especificamente no dia 04 de ABRIL de 2013, passou a vigorar a Lei nº 12.737, de 30 de novembro 2012, popularmente denominada "Lei Carolina Dieckmann".

A conduta de invadir dispositivo informático, à época do fato não era considerada crime, porém, com a promulgação da novel legislação que acrescentou dois artigos ao Código Penal Brasileiro, 154 – A e 154 – B, sendo que o primeiro versa sobre delito de invasão de dispositivo[60].

Por se tratar de legislação recente, não há notícia de aplicação ou constatada eficácia. Todavia, antes mesmo da tipificação do crime de invasão de dispositivo informático, a doutrina já tratava tal conduta como ilícita. Todavia, enquadrava-se em outras condutas tipificadas no Código Penal, conforme comentários acerca da pratica de tal delito, expressos na doutrina de Marcelo Xavier de Freitas Crespo, em data anterior a entrada em vigor da referida Lei.

> Deve-se mencionar que o ordenamento brasileiro ainda não incriminou, em termos gerais, a conduta de "acesso não autorizado de sistemas informáticos". Mesmo assim, é forçoso reconhecer o caráter ilícito de se acessar sem autorização um sistema informático. Todavia, parece não se ter consenso sobre qual o bem jurídico afetado, apesar de que recomendações de organismos internacionais sejam no sentido de tratá-lo como delito econômico. A nosso ver, no entanto, não se pode vincular em absoluto o caráter econômico a tal conduta, haja vista nem sempre se verificar o ânimo de lucro ou prejuízo patrimonial.[61]

---

[59] CRESPO, Marcelo Xavier de Freitas. Crimes Digitais. 1 ed. 2ª tiragem, Saraiva: São Paulo, 2011. p. 64.

[60] Lei nº 12.737/2012. 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.

[61] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1 ed. 2ª tiragem, Saraiva: São Paulo, 2011. p. 66.

Com tais considerações, resta claro que mesmo antes da existência de lei específica, já era reconhecido, ainda que de forma tímida o caráter ilícito do acesso não autorizado a sistema informático.

Por tanto, a Lei 12.737/2012, trata-se de novidade no universo jurídico nacional e, vem de encontro com uma necessidade antiga dos brasileiros, que agora têm respaldo do poder judiciário e poderão ver punido aquele que lhe causou mau através do meio cibernético.

2.2.2 – Dano Informático

O Código Penal Brasileiro em seu Capítulo IV, especificamente no artigo 163[62], trata do crime de dano, que traz os verbos: destruir, inutilizar ou deteriorar coisa alheia. Quanto a esse delito, importante valer-se dos ensinamentos de Rogério Greco:

> O art. 163 do Código Penal. em sua modalidade fundamental. comina pena de detenção, de 1 (um) a 6 (seis) meses. ou multa, para aquele que destruir, inutilizar ou deteriorar coisa alheia. Assim, podemos destacar os seguintes elementos que compõem o delito de dano: a) a conduta de destruir, inutilizar ou deteriorar; b) que qualquer um desses comportamentos tenha como objeto a coisa alheia. O núcleo destruir é empregado no texto legal no sentido de eliminar, aniquilar, extinguir; inutilizar significa tornar inútil. imprestável a coisa para os fins originais a que era destinada, mesmo que não destruída; deteriorar é estragar, arruinar a coisa.[63]

O Código Penal brasileiro prevê pena de detenção ou multa para aquele que destruir, inutilizar ou deteriorar coisa alheia. Um dos aspectos é que qualquer destes verbos tenha como objeto a coisa alheia, não esclarecendo, todavia, o que é a coisa alheia, se é simplesmente bem material ou abrange também os imateriais, quanto a isso, ensina Marcelo Xavier de Freitas Crespo, disciplinando o tema no contexto do direito criminal digital, sobre a possibilidade da aplicação ou não do referido dispositivo nos danos causados a dados informáticos.

> O cerne da questão está no objeto material do crime, ou seja, "coisa", A doutrina não discute a aplicação do art. 163 quanto à mobilidade do objeto, sendo pacífica a aceitação do ilícito dirigido contra coisas móveis ou imóveis. Todavia, as divergências surgem quando se menciona o aspecto material/imaterial das coisas. Até esse ponto, não há dúvidas de que o dano é crime possível contra coisas materiais, de forma que objetos como o próprio computador, seu monitor, uma impressora, um *scanner*, são todos coisas materiais, dotados de valor econômico, de modo que podem tranquilamente ser objetos de crime de dano.[64]

---

[62] Lei nº 12.737/2012. Art. 163. Destruir, inutilizar ou deteriorar coisa alheia: Pena – detenção, de (um) a 6 (seis) meses, ou multa.
[63] Greco, Rogério. **Código Penal: comentado** - 5. ed. - Niterói, RJ: Impetus, 2011. p.478.
[64] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1 ed. 2ª tiragem, Saraiva: São Paulo, 2011. p. 71.

Com as considerações acima, a problemática que se apresenta neste contexto paira em torno da aplicabilidade ou não da norma para os danos causados a bens imateriais, como arquivos gravados em um *hard disc*[65], uma vez que, embora se possa tocar a mídia onde se encontram os arquivos, o conteúdo que está gravado é imaterial, de forma que se pode apagá-lo sem causar dano algum ao equipamento físico.

Para Marcelo Xavier de Freitas Crespo, não é possível considerar típico o crime de danos a dados informáticos, uma vez que não há tese capaz de vencer o devido repeito ao princípio da legalidade. Ainda, aduz que caso alguém, sem autorização do proprietário e visando exclusivamente causar prejuízo a outrem, apague os dados constantes no *hard disc*, não haveria que se falar em crime de dano, tendo em vista que nenhuma coisa foi destruída, inutilizada ou deteriorada, vez que se entende o termo "coisa" como algo material.[66]

2.2.3 – Dos Vírus e sua disseminação

Definidos como, seguimentos de códigos, que se anexam a programas ou arquivos, são pré-programados para realizarem determinadas ações, bem como se propagarem pelas máquinas e contaminarem outros sistemas em contato com esta, através de e-mails remetidos automaticamente ou mesmo transmissão de dados, por qualquer outra forma e, assim como os vírus que atacam os seres humanos, os vírus de computadores, variam quanto ao grau de dano causado, podendo ocasionar um mero inconveniente, ou mesmo gerar a perda total de dados.[67]

Em termos simples, o vírus nada mais é que um comando realizado através de códigos, que atribui ao vírus uma determinada função, de forma que ele realizara unicamente aquela tarefa para a qual foi criado, não sofrendo mutações, a menos que outra pessoa altere os códigos para que seja realizado outro comando.

Dentre os vírus existentes pode-se apontar alguns mais conhecidos, como o vírus de *boot* e o vírus *time bomb*. Todo disco possuí um setor de inicialização do sistema, sendo que a principal característica do vírus *boot* é que ele se fixa nesse setor, vírus estes que em sua maioria são autorreplicantes, ou seja, criam cópias de si mesmos em outras mídias que são inseridas no equipamento disseminando assim rapidamente. Já os vírus *time bomb*, destinam-se a realizar

[65] Termo da língua inglesa que denomina o disco rígido ou disco duro, local destinado ao armazenamento de dados.
[66] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1 ed. 2ª tiragem, Saraiva: São Paulo, 2011. p. 72.
[67] Ibidem . p. 74.

um determinado evento em uma data específica previamente programado por aquele que o criou, são exemplos deste vírus, o *sexta-feira 13*[68]*, 1º de abrli*[69]*,* dentre outros[70].

Diante dos vários crimes digitais por meio de ataques, pode-se destacar os *malwares*, que são *softwares* mal intencionados, destinados a infiltrar em computadores alheios.

> Dentre os malwares encontram-se os vírus, segmentos de códigos de computação que se anexam a programas ou sistemas de modo a se propagar pelas máquinas e contaminar outros sistemas em contatos com esta, através de e-mails remetidos automaticamente e até mesmo por transmissão de dados maliciosos por outros métodos. Sua criação se dá com o intuito de explorar falhas de segurança e multiplicá-las, o que geralmente se dá com o auxílio humano através da circulação de arquivos que as contenham.[71]

Embora se trate de um *software* mal intencionado, verifica-se que dificilmente um vírus trará prejuízos financeiros, a não ser aqueles casos em que se faz necessário assistência técnica para recuperar um sistema infectado, que pode tornar-se muito lento ou mesmo ser corrompido. Porém, em grande parte das vezes, os vírus tem por objeto direcionar o usuário para uma determinada página na internet, ou exibir imagens engraçadas ou pornográficas. Embora possa servir de meio para realização de outros crimes, não há previsão legal para quem crie ou dissemine os vírus cibernéticos.

Ainda, em que pese não haver legislação específica para punir aqueles que criam e disseminam vírus, levando em conta as perturbações e transtornos causados por conta destas pragas virtuais, a conduta referente à criação de disseminação pode amoldar-se ao art. 65 da Lei das contravenções penais[72].

2.2.4 – Engenharia Social e *Phishing*

Mesmo que, recentemente tenha ganhado a denominação de engenharia social, trata-se de termo que há muito tempo já é conhecido no direito penal, porém com nomenclatura adversa, qual seja, artifício fraudulento. Pode-se entender como engenharia social todo método

---

[68] Tipo de vírus programando para executar na sexta feira 13, que apagava o conteúdo do HD ou inutilizava o micro de alguma forma.
[69] Vírus que infestou milhares de máquinas pelo mundo e ganhou destaque no dia 1º de abril, os intrusos poderiam roubar dados e assumir o controle dos computadores infectados.
[70] WENTED, Emerson. JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport, 2012. p. 23 e 24.
[71] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1 ed. 2ª tiragem, Saraiva: São Paulo, 2011. p. 74.
[72] DECRETO-LEI nº 3.688, de 3 de outubro de 1941. Art. 65. Molestar alguem ou perturbar-lhe a tranquilidade, por acinte ou por motivo reprovável:Pena – prisão simples, de quinze dias a dois meses, ou multa, de duzentos mil réis a dois contos de réis.

de mascarar a realidade, para enganar alguém que detém dados importantes, a fim de tê-los para si. Trata-se de um artifício intelectual para chegar a determinadas informações sigilosas e pode ocorrer através de qualquer meio de comunicação[73].

Ponto que diferencia a engenharia social e o *Phishing* dos demais delitos informáticos, é que neste tipo de crime o agente ativo utiliza-se de vulnerabilidades da vítima e não das falhas dos sistemas informáticos. Certo é que as vítimas deste delito são carentes de informações, eis que o autor do delito utiliza-se da persuasão para conseguir aquilo que quer.

> Enquanto certas ameaças cibernéticas utilizam vulnerabilidades localizadas em uma rede ou servidor, na engenharia social o criminoso concentra-se nas vulnerabilidades que porventura a vítima possa ter e/ou apresentar frente a determinadas situações do seu cotidiano. Nestas situações o ponto nevrálgico é a falta de conscientização do usuário de computador sobre os perigos de acreditar em todas as informações que chegam até ele.[74]

Assim, chega-se à conclusão de que neste tipo de crime é sempre observado o despreparo da vítima para utilizar o computador, fornecendo dados pessoais a terceiros, sem haver plena convicção de quem realmente irá receber estes dados sigilosos, ou seja, neste tipo de crime, o agente ativo faz uso da persuasão, aproveitando-se da ingenuidade da vítima para obter aquilo que almeja.

O principal meio de se consumar a engenharia social é o *phishing*, que deriva do vocábulo *to fish* ou *fishing*, que significa pescar, sendo que a finalidade é obter informações relevantes na modalidade fraude virtual.

O *fhishing* ocorre da seguinte forma: o agente ativo do crime envia uma mensagem, podendo ser um e-mail ou até mesmo um recado na página de relacionamentos do agente passivo, utiliza todo seu intelecto para ludibriar e induzir a pessoa a fornecer dados que lhe são pertinentes, como números de contas bancárias, cartões de créditos, documentos pessoais e outros, ou a baixar e executar programas que auxiliem o roubo destas informações posteriormente.[75]

Dadas as características deste delito, pode-se concluir que é uma espécie de estelionato, só que, praticado no ambiente virtual. Quanto ao crime de estelionato, veja-se o que diz Rogério Greco:

> Sendo a fraude o ponto central do delito de estelionato, podemos identificá-lo. Outrossim, por meio dos seguintes elementos que integram sua figura típica: a) conduta do agente dirigida finalisticamente à obtenção de vantagem Ilícita, em prejuízo alheio; b) a vantagem ilícita pode ser para o próprio agente ou para terceiro;

---

[73] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1 ed. 2ª tiragem, Saraiva: São Paulo, 2011. p. 82.
[74] WENTED, Emerson. JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport, 2012. p. 20.
[75]CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1 ed. 2ª tiragem, Saraiva: São Paulo, 2011. p. 83.

> c) a vítima é induzida ou mantida em erro; d) o agente se vale de artifício, ardil ou qualquer outro meio fraudulento para a consecução do seu fim. [76]

Ante o acima relatado, resta clara a similitude entre o estelionato e a engenharia social ou *phishing*, uma vez que a obtenção de senhas, numerais e códigos, leva, ou ao menos tem o intento de levar vantagem econômica por parte do agente ativo do crime que através da engenharia social e de artifícios ardilosos tecnológicos busca induzir o usuário ao erro[77].

Embora já tenha sido objeto de projeto de Lei[78] cuja redação visava acrescentar novo inciso ao parágrafo § 2º do art. 171 do código penal para tratar especificamente do estelionato eletrônico, em nosso ordenamento jurídico não há norma específica para o *phishing*, sendo que só quando verificados todos os quesitos necessários para configuração do crime de estelionato "fraude, artifício ou ardil" + "vantagem indevida" + "prejuízo alheio", pode-se enquadrar o fato em tal dispositivo.

2.2.5 – Interceptação Ilegal de dados

Em nossa Constituição Federal de 1988, mais especificamente no art. 5º, XII[79], foi atribuído à inviolabilidade das telecomunicações em geral, caráter de direito fundamental.

Ademais, além de trazer a salvo a garantia da inviolabilidade, pode-se verificar a interceptação telefônica, telemática ou informática sem autorização judicial ou em desconformidade com a lei, configura crime, nos termos do art. 10 da Lei 9.296/96, dispositivo este que visa incriminar a interceptação ilegítima, com intuito de cumprir a convenção de Budapeste[80].

Dessa forma, tendo em vista que a cada dia a sociedade torna-se ainda mais dependente dos meios eletrônicos, dos computadores, celulares e principalmente da internet, necessário se

---

[76] GRECO, Rogério. **Código Penal: comentado** - 5. ed. - Niterói, RJ: Impetus, 2011. p. 513.
[77] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1 ed. 2ª tiragem, Saraiva: São Paulo, 2011. p. 85.
[78] PL 84/1999
[79] "Art. 5º (...) 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 processual penal."
[80] "Art. 3º - Intercepção Ilegítima. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, a intercepção intencional e ilegítima de dados informáticos, efectuada por meios técnicos, em transmissões não públicas, para, de ou dentro de um sistema informático, incluindo emissões electromagnéticas provenientes de um sistema informático que veicule esses dados. As Partes podem exigir que a infracção seja cometida com dolo ou que seja relacionada com um sistema informático conectado com outro sistema informático".

faz uma maior proteção jurídica voltada para o campo cibernético, visando resguardar as pessoas e os bens que podem ser alvos de delitos cometidos neste meio.

2.3 – Dos Delitos Informáticos Impróprios

Nesta classe, estão os crimes que já existiam no ordenamento jurídico, especialmente no Código Penal porém com a adaptação ao meio de praticar, ou seja, através dos meios eletrônicos, de forma que os crimes já tradicionalmente previstos em nossa legislação podem ser cometidos por meio de novos *modus operandi*[81].

Os delitos informáticos impróprios, pouco se diferenciam dos crimes comuns, previstos na parte especial do Código Penal Brasileiro. A dicotomia encontra-se apenas do meio pelo qual o agente realiza sua atividade criminosa. Porém a dificuldade de encontrar o criminoso que age através de computadores é maior, uma vez que necessita investigação mais sofisticada bem como a realização de perícia técnica, para comprovar a autoria do fato.

Dentre os vários delitos que podem ser cometidos por meio virtual, elenca-se os mais corriqueiros, iniciando com a pornografia infantil, tipo de crime que causa grande fervor na sociedade e que com a popularização dos computadores e internet tem aumentado de forma considerável o índice de ocorrências o que pode ser verificado até mesmo através dos meios de comunicação, que diariamente noticiam a ocorrência desse tipo de delito.

2.3.1 – Pornografia infantil

A princípio, insta esclarecer a dicotomia existente entre os termos pedofilia e a pornografia infantil. Na primeira, há uma perversão sexual, onde o adulto expressa sentimentos eróticos por crianças e/ou adolescentes, é em verdade um transtorno sexual. Já na pornografia infantil não é necessária a ocorrência da relação sexual, bastando para tanto a comercialização de fotografias ou vídeos eróticos ou pornográficas envolvendo crianças e/ou adolescentes.[82]

Com a facilidade de comunicar-se em tempo real, através de voz e imagem, tecnologia esta oriunda do advento da internet, bem como envio de recebimento de arquivos, como fotos

[81] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1 ed. 2ª tiragem, Saraiva: São Paulo, 2011. p. 87.
[82] INELLAS, Gabriel Cesar Zaccaria de. **Crimes na Internet**. São Paulo: Editora Juarez de Oliveira, 2004. p.46

e vídeos, para qualquer local do mundo, é natural que criminosos utilizem destes meios para prática de condutas delitivas. É o caso daqueles que publicam, distribuem, armazenam fotos, vídeos e imagens de cunho sexual, envolvendo crianças ou adolescentes.

> Segundo as pesquisas, chega a 7 milhões o número de meninas e meninos vítimas de assédio sexual. Neste quadro devastador, há cerca de 6 mil páginas envolvendo crianças e adolescentes em situação sexual, sendo que 80% do tráfico de imagens se encontra no Orkut, onde se encontra um meio fácil de divulgação da pedofilia, através de suas comunidades, movimentando milhões de dólares em todo o mundo, Cada filme envolvendo crianças custa, em média, U$ 400,00 e o preço das fotografias varia de U$ 100,00 a U$ 200,00.[83]

Viu-se que a tecnologia facilitou e muito a prática de crimes deste gênero, uma vez que os criminosos desta modalidade podem estar em redes sociais, blogs, sites e etc. Ademais, em que pese os dados acima referirem-se ao ano de 2006, nota-se que já se havia um número expressivo, o que com a popularização da internet e dos computadores, gera um consequente aumento nestas práticas criminosas.

Importante esclarecer que grande parcela das pessoas utilizam de forma errônea o termo "pedofilia" para se referir aos crimes de armazenamento e divulgação de material pornográfico envolvendo crianças ou adolescentes. Desse modo, necessário se faz utilizar de maneira correta o termo.

Muitas pessoas, inclusive aquelas que dispões de formação técnica equivocam-se ao denominar "pedofilia" os crimes relativos à divulgação e armazenamento de imagens com conteúdo de pornografia infantil, incorrem também no erro de referir-se a relação sexual entre maiores e menores de idade de "pedofilia". O conceito técnico de pedofilia diz respeito a um transtorno da preferência sexual, uma parafilia[84], de forma que não há crime no Brasil com essa denominação. A lei, em verdade, pune os diversas situações que envolvam menores em exposição de sexualidade infantil, seja fotos, imagens, filmagens e interpretações teatrais, bem como, é crime transmitir, publicar, distribuir, adquirir, possuir e armazenar, vídeos, imagens, fotografias que envolvam situações pornográficas com crianças e adolescentes.[85]

Assim, pode-se entender que pedofilia não é o crime em si, mas sim um transtorno de preferência sexual, pelo que resta esclarecido que se trata *de* um erro de nomenclatura referir-se a prática do crime de produção, reprodução, registro ou outra forma que exposição com cunho sexual que envolva crianças ou adolescentes.

---

[83] MUOIO, Arlete Figueiredo. AGUIAR, Malu. **Crimes na Rede: O Perigo que se Esconde no Computador**. Companhia Ilimitada: São Paulo, 2006. p. 142 e 143.
[84] Transtorno sexual recorrente.
[85] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1 ed. 2ª tiragem, Saraiva: São Paulo, 2011. p. 90.

Conforme dispõe a Lei 8069/1990 (Estatuto da Criança e do Adolescente), em seu art. 2º[86], criança é quem tem até doze anos incompletos e, adolescentes é aquele com idade compreendida entre doze a dezoito anos. Ainda, o art. 240[87] da mesma Lei, assevera que, aquele que produzir, reproduzir, dirigir, fotografar, filmar ou registrar, cena de sexo explícito ou pornográfico, envolvendo criança ou adolescente incorre em crime.

Para chegar até o agente que praticou alguma das condutas previstas nos artigos supramencionados, muitas das vezes é necessária a quebra de sigilo, para que se possa rastrear a fonte, isto é o dispositivo de onde veio o arquivo, e após conseguir localizar o indivíduo, as provas deverão ser analisadas por peritos técnicos, a fim de comprovar a real autoria do fato, para que sejam aceitas em juízo.[88]

2.3.2 – Violação de Direitos autorais

A violação dos direitos autorais, também conhecida como pirataria, constitui o ato de copiar ou vender produto sem o consentimento do detentor dos direitos autorais. Até mesmo o uso de marcas e documentos encontrados com auxílio da internet podem configurar crime. O objeto protegido pela lei brasileira é a propriedade intelectual, que subdivide-se em dois grupos, a propriedade industrial, que refere-se às patentes, ao desenho industrial, às marcas e aos nomes de domínio e, o outro grupo é o dos direitos autorais que diz respeito *softwares*, banco de dados, documentos técnicos e outros.[89] Na internet a fiscalização é precária, bem como a ausência de territorialidade, o que simplifica para que as informações viagem de forma veloz, o que dificulta a identificação de sua origem. Ainda, permite também que sejam feitas cópias de materiais disponibilizados, de forma desordenada, onde grande parte das vezes o criador é desrespeitado,

---

[86] **Art. 2º** Considera-se criança, para os efeitos desta Lei, a pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade.

[87] **Art. 240**. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente: Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa. § 1o Incorre nas mesmas penas quem agencia, facilita, recruta, coage, ou de qualquer modo intermedeia a participação de criança ou adolescente nas cenas referidas no caput deste artigo, ou ainda quem com esses contracena. § 2o Aumenta-se a pena de 1/3 (um terço) se o agente comete o crime: I – no exercício de cargo ou função pública ou a pretexto de exercê-la; II – prevalecendo-se de relações domésticas, de coabitação ou de hospitalidade; ou III – prevalecendo-se de relações de parentesco consangüíneo ou afim até o terceiro grau, ou por adoção, de tutor, curador, preceptor, empregador da vítima ou de quem, a qualquer outro título, tenha autoridade sobre ela, ou com seu consentimento.

[88] PINHEIRO, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.p.300 - 301.

[89] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1 ed. 2ª tiragem, Saraiva: São Paulo, 2011. p. 89.

tendo em vista que não são assegurados seus direitos como autor da obra que está sendo replicada[90].

O fato de algo estar disponível na internet não significa que seja público ou que possa ser usado por qualquer pessoa, sem a citação da fonte, o ato de violar direito autoral, constitui crime.

> Assim, é crime violar direitos de autor de programa de computador, bem como a venda, aquisição, exposição à venda, o depósito ou a ocultação, para fins de comércio, de original ou cópia de programa de computador, produzido com violação de direito autoral. É o que dispõe a Lei n. 9.609/98. As violações que não sejam relativas a *software* são punidas nos termos do art. 184 do Código Penal. Por fim, as violações à propriedade industrial são punidas nos termos da Lei n. 9.279/96. Vale mencionar o *Creative Commons*, que é um conjunto de licenças padronizadas que permite aos autores disponibilização mais fácil de suas obras, caso desejem renunciar a parte de seus direitos. Isso auxilia a circulação das obras sem que a todo momento seja preciso pedir autorização e licença aos autores.[91]

Ou seja, nos termos da Lei 9.609/98, aquele que violar direitos autorais, vender ou expor a venda estará incorrendo em crime, eis que, no Brasil há legislação específica que incrimina a violação de direitos autorais de programa de computador, e em seu art. 12, dispõe acerca da ilegalidade da conduta de violar direitos autorais[92].

Para facilitar a questão dos direitos autorais, existe o *Creative Commons*, que é um tipo de licença padronizada, dentre as licenças, tem-se a "Atribuição (by)", licença permite que outros distribuam, remixem, adaptem ou criem obras derivadas, mesmo que para uso com fins comerciais, contanto que seja dado crédito pela criação original. Esta é a licença menos restritiva de todas as oferecidas, em termos de quais usos outras pessoas podem fazer de sua obra.

Dentre outras, vislumbra-se ainda a "Atribuição – Uso Não Comercial – Não a Obras Derivadas (by-nc-nd)" que é a licença mais restritiva dentre as seis licenças principais, permitindo redistribuição. Ela é comumente chamada "propaganda grátis", pois permite que

---

[90] PINHEIRO, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.p.134.

[91] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1 ed. 2ª tiragem, Saraiva: São Paulo, 2011.p. 89 - 90.

[92] **Art. 12.** Violar direitos de autor de programa de computador: Pena - Detenção de seis meses a dois anos ou multa. § 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente: Pena - Reclusão de um a quatro anos e multa. § 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral. § 3º Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo: I - quando praticados em prejuízo de entidade de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo poder público; II - quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo. § 4º No caso do inciso II do parágrafo anterior, a exigibilidade do tributo, ou contribuição social e qualquer acessório, processar-se-á independentemente de representação.

outros façam download das obras licenciadas e as compartilhem, contanto que mencionem o autor, mas sem poder modificar a obra de nenhuma forma, nem utilizá-la para fins comerciais.[93]

2.3.3 – Crimes contra a honra

A Constituição Federal, em seu art. 5º, X, estabelece que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". Desse modo, aplica-se também a punição criminal, para aquele que deliberadamente, ofende a honra de outrem.

Um bem protegido pela legislação brasileira, que diz respeito aos atributos da pessoa, os seus valores, a forma como é vista na sociedade, tudo isso diz respeito à honra.

> Honra são as qualidades físicas, morais e intelectuais de uma pessoa, fazendo-a respeitada no meio social e que diz respeito, ainda, à sua autoestima.
> A honra representa verdadeiro patrimônio moral, merecedor de proteção, porque revela o valor social da pessoa, importando sua aceitação ou rejeição.[94]

Tendo o reconhecimento jurídico de sua importância, a ofensa à honra constitui crime. Em relação aos crimes contra honra, discorre Vitor Eduardo Rios Gonçalves:

> Os crimes contra a honra são a calúnia, a difamação e a injúria. Cada um desses delitos tem requisitos próprios e, além de estarem descritos no Código Penal, estão também previstos em leis especiais, como o Código Eleitoral, o Militar e a Lei de Segurança Nacional. Desse modo, os tipos penais da legislação comum só terão vez se não ocorrer quaisquer das hipóteses especiais[95].

Trazendo para o enfoque do trabalho, os crimes contra a honra estão previstos nos artigos 138, 139 e 140 do Código Penal, são delitos bastante corriqueiros no mundo virtual. Considerando o grande número de pessoas que utilizam os vários serviços ofertados na internet, neste caso, principalmente as redes sociais, local onde ocorre grande parte dos crimes contra a honra no ambiente cibernético.

Insta constatar, assim, que a honra, é bem de extrema relevância, eis que sua inviolabilidade encontra-se expressa em nossa Constituição Federal, bem como há previsão

---

[93] AS LICENÇAS, **Creative Crommons**, disponível em <http://creativecommons.org.br/as-licencas/>, acesso em 28/04/2013.
[94] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1 ed. 2ª tiragem, Saraiva: São Paulo, 2011. p. 90.
[95] GONÇALVES, Victor Eduardo Rios. **Direito penal esquematizado: parte especial** – São Paulo : Saraiva, 2011. p. 234.

legal dos crimes contra a honra em nosso em nosso diploma criminal, que tipificou como crime, a calúnia, a difamação e a injúria.

2.3.3.1 – Calúnia

O crime de calúnia encontra-se previsto no art. 138 do Código Penal Brasileiro e está assim disposto "Caluniar alguém imputando-lhe falsamente fato definido como crime. Neste crime, a honra da vítima é abalada ao ter atribuído contra si fato definido como crime, manchando sua reputação perante a sociedade.

Para configurar tal delito, necessário se faz que o agente atribua a uma determinada pessoa, o exercício de conduta determina em lei como crime e que saiba ser mentirosa tal atribuição, sendo que, caso o agente esteja de boa fé, supondo de forma errônea que a conduta seja verdadeira, a intenção de prejudicar a vítima estará excluída, excluindo-se também o crime.[96]

Segundo ensina Cleber Masson, o núcleo do tipo é "caluniar", isto é imputar, motivo pelo qual não era necessário dizer: "caluniar alguém, imputando-lhe..." A conduta de atribuir a alguém a prática de um determinado fato, o qual deve, entretanto, ter previsão legal como crime.

Há de ser tipificado como fato criminoso, qualquer que seja a sua espécie: seja cometido por dolo ou culpa, punido com reclusão ou com detenção, de ação penal pública (incondicionada ou condicionada) ou de ação penal privada. Bem como não há óbice que a calúnia possa se verificar mediante a imputação de um crime também de calúnia. Além disso, é imprescindível a imputação da prática de um fato determinado, isto é, de uma situação concreta, onde mencione o autor e o fato. Nesse sentido, não basta chamar alguém de "ladrão", pois si isso não é suficiente para caracterizar o crime de injúria.

Para que se configure, o crime de calúnia é necessário que o agente ativo aponte o autor do fato (pessoa caluniada) e atribua a ele fato descrito pela legislação como crime, de forma que aquele que receba a notícia possa ter convicção de que se trata de fato criminoso.[97]

Assim, relacionando o cometimento de tal crime com o universo digital, pode-se tomar como exemplo o caso de um indivíduo enviar e-mail ou publicar em redes sociais informações

---

[96] GONÇALVES, Victor Eduardo Rios. **Direito penal esquematizado: parte especial** – São Paulo : Saraiva, 2011. p. 90.
[97] MASSON, Cleber Rogério. **Direito penal esquematizado: parte especial I** - 3. ed. - Rio de Janeiro: Forense; São Paulo: MÉTODO, 2011. vol.2. p. 168.

imputando crime a determinada pessoa, sendo necessário para tanto, o preenchimento de todos os requisitos acima mencionados.

2.3.3.2 – Difamação

Conforme dispõe o art. 139 do Código Penal: "Difamar alguém, imputando-lhe fato ofensivo à sua reputação", ou seja, fato ofensivo que venha a denegrir a imagem da vítima.

Diferente da calúnia, na difamação, embora exista a imputação de determinado fato, este fato não pode ser previsto como crime, sob pena de incorrer no primeiro crime mencionado. Trata-se do fato de atribuir fato ofensivo a reputação de alguém, sendo que a lei não exige para tanto, que o fato seja falso, bastando apenas a atribuição de fato desonroso.[98]

No mesmo sentido é a lição de Vitor Eduardo Rios Gonçalves:

> Conforme indica o próprio nome do delito, difamar significa causar má fama, arranhar o conceito de que a vítima goza perante seus pares, abalar sua reputação.Tal como ocorre na calúnia, a difamação pressupõe que o agente atribua à vítima um fato determinado, concreto, que, aos olhos de outrem, seja algo negativo. O que distingue os dois delitos basicamente é que, na calúnia, o fato imputado necessariamente deve ser definido como crime, enquanto a difamação é genérica, isto é, abrange a imputação de qualquer outro fato ofensivo[99].

Novamente, trazendo para o contexto do presente trabalho, pode-se tomar como exemplo do crime de difamação na rede, o caso de o agente comunicar a terceiros através dos meios virtuais que determinada pessoa usa drogas ou se prostitui.

2.3.3.3 – Injúria

Nos termos do art. 140 do Código Penal constitui crime: "Injuriar alguém, ofendendo lhe a dignidade ou o decoro", neste tipo verifica-se como sendo um bem tutelado os atributos morais intelectuais ou físicos, que quando denegridos por um terceiro, incorre-se no crime de injuria.

---

[98] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1 ed. 2ª tiragem, Saraiva: São Paulo, 2011. p. 91.
[99] GONÇALVES, Victor Eduardo Rios. **Direito penal esquematizado: parte especial** – São Paulo : Saraiva, 2011. p. 243.

> Injuriar é ofender, falar mal, insultar, sem necessidade de atribuir a alguém um fato determinado. Assim, porque a ofensa é dirigida á honra subjetiva, o crime só ocorre caso a vítima tome conhecimento da ofensa, ainda que por terceiro.[100]

Dessa forma, necessário se faz que o insulto chegue até a vítima, isto é, que a pessoa tome conhecimento do fato a ela dirigido e fique insatisfeita, isto é injuriada, corroborando, é a lição de Vitor Eduardo Rios Gonçalves:

> A injúria difere totalmente dos outros crimes contra a honra porque é o único deles em que o agente não atribui um fato determinado ao ofendido. Na injúria, o agente não faz uma narrativa, mas atribui uma qualidade negativa a outrem. Consiste, portanto, em um xingamento, no uso de expressão desairosa ou insultuosa para se referir a alguém. A característica negativa atribuída a alguém, para configurar injúria, deve ser ofensiva à sua dignidade ou decoro[101].

Com essas considerações, tem-se que o crime de injúria se diferencia dos outros, eis que, nessa modalidade de crime contra a honra, não é atribuído nenhum fato a vítima, mas sim um xingamento, alguma palavra que insulte a moral ou a honra da pessoa.

Assim, trazendo para o ambiente virtual, verifica-se a ocorrência do crime de injuria quando por meio de comunicação eletrônico, o agente comenta características negativas em relação a vítima, todavia, o crime só se consuma quando o comentário chegar ao conhecimento da pessoa para qual foi dirigido.

---

[100] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1 ed. 2ª tiragem, Saraiva: São Paulo, 2011. p. 91.
[101] GONÇALVES, Victor Eduardo Rios. Direito penal esquematizado: parte especial – São Paulo : Saraiva, 2011. p. 247.

CAPÍTULO III. DA PERSECUÇÃO CRIMINAL: PROVAS NOS DELITOS INFORMÁTICOS

3.1 Da investigação preliminar à propositura da ação penal

O procedimento criminal para análise da prática de um delito é caracterizado por duas fases, a investigação criminal e do processo penal. Cronologicamente, a primeira fase é a investigação criminal, cuja competência é da polícia judiciária civil, cabendo a ela levantar os principais fatos, relativamente à ocorrência, visando elucidar a materialidade, isto é no acontecimento do delito e a autoria, o agente criminoso.[102]

Essa investigação criminal, realizada pela polícia civil é um procedimento administrativo, de caráter preliminar, que tem por objetivo reunir as provas que forem possíveis para a formação do juízo do promotor de justiça, revelando-se a justa causa para propositura da ação penal. Esta primeira fase é de fundamental importância, de forma que, se a investigação for bem feita, com a produção de provas concretas, tornará mais coesa a decisão do magistrado.

É oportuna a ressalva, de que nem todas as condutas típicas são tuteladas pelo direito penal, ou seja, ainda que esteja comprovada autoria e materialidade do delito, há de se verificar a existência de justa causa para propositura da ação penal. Noutras palavras, o caráter fragmentário do Direito Penal significa que o Direito Penal não deve sancionar todas as condutas lesivas aos bens jurídicos tutelados pela norma penal, mas tão somente as condutas mais graves e perigosas cometidas contra os bens mais caros à sociedade.

Na etapa da investigação preliminar ainda não há um processo judicial, mas tão somente a verificação do preenchimento das condições para a propositura da ação penal, quais sejam: *fumus commissi delicti* e *periculum libertatis*. Não há, portanto, imposição direta de nenhum tipo de penalidade, sendo o momento de apuração das circunstâncias que levam a crer, em cognição sumária, a existência de indícios suficientes de autoria e materialidade do cometimento do delito e, para os casos em que haja pedido de prisão preventiva ou cautelar, a justificação de risco à ordem pública com a liberdade do agente.

> Trata-se de procedimento de natureza administrativa. Não se trata, pois, de processo judicial, nem tampouco de processo administrativo, porquanto dele não resulta a

[102] GRANZOTTO, Claudio Geoffroy. **Análise da investigação preliminar de acordo com seus possíveis titulares**. Jus Navigandi. Disponível em: <http://jus.com.br/artigos/9522/analise-da-investigacao-preliminar-de-acordo-com-seus-possiveis-titulares#ixzz2gdGktOaC> Acesso em 03/10/2013, às 02h10min.

> imposição direta de nenhuma sanção. Nesse momento, ainda não há o exercício de pretensão acusatória. Logo, não se pode falar em partes stricto sensu, já que não existe uma estrutura processual dialética, sob a garantia do contraditório e da ampla defesa.[103]

Até este momento, ainda não há uma formação processual, existe apenas a formação do inquérito policial, que dará subsídios para o trâmite de uma futura ação penal.

Quanto às peculiaridades que dizem respeito à persecução criminal, nos delitos informáticos, lembram Emerson Wented e Higor Vinícius Nogueira Jorge[104], que a investigação pode ser dividida em duas fases: fase técnica e fase de campo.

Quanto a essa divisão, discorrem os referidos autores aduzindo que a primeira fase da investigação, a fase técnica tem o objetivo de localizar o computador que foi utilizado para o cometimento do delito, devendo para tanto serem tomados alguns cuidados. Primeiro deles diz repeito à orientação da vítima, de forma a preservar as provas presentes no computador para, coleta inicial, o que deve ser estritamente observado, principalmente no caso da necessidade de quebra de sigilo de dados, o que deve ser autorizado pela autoridade judiciária, sob pena de nulidade da prova, conforme visto anteriormente.

É também nesta fase que se realiza a busca aos dados disponíveis na internet, como prováveis autores, origem de e-mails, registro de hospedagem de domínio e etc. Tudo isso, com o objetivo principal de descobrir o equipamento utilizado para execução do crime, objeto principal da fase técnica.

Após localizado o equipamento informático que permitiu a conexão e o acesso criminoso na internet, passa-se para a próxima fase da investigação, fase de campo. Momento em que os agentes policiais efetuam diligências para efetuar o reconhecimento operacional do local[105].

Essas diligências deverão ocorrer de maneira discreta, pois, poderá haver a necessidade de solicitar uma medida judicial cautelar, como pedido de busca a preensão, caso em que será deferido pelo juízo, quando verificado que o endereço pertence a uma casa ou a uma rede não corporativa[106]. Cabe aos investigadores agirem com diligência e cautela, de forma a não levantarem suspeita dos investigados quanto à realização das investigações relativas a eles, para que não possam destruir, inutilizar ou dificultar uma possível colheita das provas nos dispositivos informáticos.

---

[103] Lima, Renato Brasileiro de. **Manual de processo penal**, vol. l - Niterói, RJ: Impetus, 2011 .p.114.
[104] WENTED, Emerson. JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport, 2012. P. 52.
[105] Ibidem. p. 53.
[106] Ibidem. p. 54.

É indispensável a autorização judicial para que se efetive a quebra de sigilo de dados bem como para que ocorra a busca e apreensão de equipamentos informáticos, sob pena de nulidade da prova obtida. Na hipótese de busca e apreensão, ainda, deve o mandado conter, pormenorizadamente, a exata localização e descrição do bem objeto de busca e apreensão, a fim de que não recaia sobre instrumento informático diverso daquele inicialmente perseguido pela autoridade judiciária.

Com a conclusão das fases técnica e de campo, encerra-se a fase inquisitorial e, se preenchidos os requisitos mínimos, caberá ao representante do *parquet* oferecer a denúncia ao poder judiciário, competente para conhecer a ação penal, que é definida por Alexandre Cebriam Araújo Reis e Vitor Eduardo Rios Gonçalves, como "o procedimento judicial iniciado pelo titular da ação quando há indícios de autoria e de materialidade a fim de que o juiz declare procedente a pretensão punitiva estatal e condene o autor da infração penal."[107]

Conforme extrai-se do trecho acima, cabe ao titular da ação penal, que, na maioria das vezes é o Ministério Público, iniciar o procedimento, através do oferecimento da denúncia, sendo defeso ao juiz iniciar de plano a ação, isto é, sem o oferecimento da denúncia, devendo ser observado o princípio da inércia.

Ainda, para a propositura da ação penal, devem ser levadas em conta algumas condições, sendo elas: legitimidade da parte, por exemplo, se ação penal pública, deve ser proposta pelo Ministério Público e, se privada, pelo ofendido ou seu representante legal, ainda, o acusado deve ser maior de 18 anos e ser imputável; Interesse de agir, que é a existência de indícios suficiente de autoria e materialidade e; possibilidade jurídica do pedido, necessitando que o fato descrito na denúncia ou queixa seja típico.

Superada a primeira fase, tem início processo penal com o recebimento da denúncia pelo Poder Judiciário.

Em não havendo absolvição sumária, bem como inexistindo hipótese de extinção da punibilidade ou da pretensão punitiva do Estado, inicia-se a segunda fase da persecução criminal, qual seja, fase de análise das provas produzidas durante a investigação preliminar, bem como a produção de novas provas.

---

[107] REIS, Alexandre Cebrian Araújo e GONÇALVES, Victor Eduardo Rios. **Direito processual penal esquematizado**. Coordenador Pedro Lenza. – São Paulo : Saraiva, 2012. p.71.

3.2 Conceito de Prova

Proposta a ação penal por intermédio da denúncia – que descreve as condutas praticadas pelo agente – e, após o recebimento pelo Poder Judiciário, começa o processo penal. Acerca dos fatos narrados pela denúncia é que irão recair as provas a serem produzidas no processo e que serão avaliadas aquelas já produzidas na investigação preliminar. Em síntese, os fatos constantes da denúncia deverão ser cabalmente comprovados pela acusação, sob pena de absolvição do réu em virtude da existência de dúvida *in dubio pro reo* ou em vista da presunção de inocência.

Com a movimentação da máquina jurídica pelo acusador, natural que seja atribuída ao réu a prática de determinado ato criminoso, motivo pelo qual se pode afirmar que a acusação estará fundada em um ou mais fatos. A conclusão do magistrado, em relação à veracidade dos fatos alegados tanto pela acusação como pela defesa, se formará com a verificação da existência dos mesmos, cuja ocorrência não é certa até o momento, visto que o recebimento da denúncia se funda em meros indícios de autoria e materialidade.

Todavia, a decisão a ser tomada pelo juiz não deve estar ligada a critérios sem fundamentos racionais, devendo ser formada através da constatação lógica oriunda dos elementos relativos ao fato, levados a ele para formar sua convicção. A prova nada mais é que esse elemento, que tem por escopo apresentar ao magistrado os subsídios necessários para formação de seu convencimento relativamente ao fato.[108]

A captura psíquica do juiz não há de ser formada – ao contrário do processo civil – em juízo de verossimilhança ou de verdade formal, mas sim em juízo de certeza acerca da ocorrência ou não da prática de determinada conduta delituosa pelo agente.

No mesmo sentido, é a lição de Fernando Capez, o qual conceitua prova da seguinte forma:

> Do latim *probatio*, é o conjunto de atos praticados pelas partes, pelo juiz (CPP, arts. 156, I e II, com a redação determinada pela Lei n. 11.690/2008, 209 e 234) e por terceiros (p. ex., peritos), destinados a levar ao magistrado a convicção acerca da existência ou inexistência de um fato, da falsidade ou veracidade de uma afirmação. Trata-se, portanto, de todo e qualquer meio de percepção empregado pelo homem com finalidade de comprovar a verdade de uma alegação. Por outro lado, no que toca à finalidade da prova, destina-se à formação da convicção do juiz acerca dos elementos essenciais para o deslinde da causa.[109]

---

[108] REIS, Alexandre Cebrian Araújo e GONÇALVES, Victor Eduardo Rios. **Direito processual penal esquematizado**. Coordenador Pedro Lenza. – São Paulo : Saraiva, 2012. p. 247.
[109] CAPEZ, Fernando. **Curso de processo penal** – 18 ed. São Paulo. Saraiva; 2011. p. 344.

Em consonância com o conceito, a prova é o conjunto de atos cuja prática depende das partes, bem como de terceiros, cujo objetivo é mostrar ao magistrado a existência ou não de um fato, comprovar a veracidade ou falsidade de uma afirmação.

Prova é, portanto, todo o meio destinado a comprovar a existência do fato referido na alegação, voltado a formação da livre convicção do juiz, para que este decida a lide pautado nos elementos constantes dos autos.

3.3 Finalidade da Prova

Em verdade, a prova destina-se a instruir o processo e formar o convencimento do juiz, uma vez que este decidirá baseado naquilo que foi levado aos autos – Noutras palavras:

> O objetivo da atividade probatória é convencer seu destinatário: o juiz. Na medida em que não presenciou o fato que é submetido a sua apreciação, é por meio das provas que o juiz poderá reconstruir o momento histórico em questão, para decidir se a infração, de fato, ocorreu e se o réu foi seu autor.[110]

Assim, tendo em vista que o juiz não presenciou os fatos que ensejaram a ação penal, devendo as partes demonstrar o ocorrido através das provas. Dessa forma, temos que a finalidade da prova é demonstrar ao magistrado, como os fatos ocorreram, valendo-se para tanto dos meios lícitos, em direito admitido.

Somente após esclarecido o acontecimento dos fatos, poderá o juiz aplicar o direito, ressaltando que a verdade almejada, é a processual, isto é, relativa, uma vez que é humanamente impossível alcançar a verdade absoluta,[111] embora o Código Penal Brasileiro tenha se pautado por este arcaico ideário.

Ainda, acerca da legalidade da prova, leciona Renato Brasileiro de Lima:

> A finalidade da prova é a formação da convicção do órgão julgador. Na verdade, da atividade probatória desenvolvida ao longo do processo, objetiva-se a reconstrução dos fatos investigados na fase extraprocessual, buscando a maior coincidência possível com a realidade histórica. Verdade seja dita, jamais será possível se atingir com absoluta precisão a verdade histórica dos fatos em questão.
> Daí se dizer que a busca é da verdade processual, ou seja, daquela verdade que pode ser atingida através da atividade probatória desenvolvida durante o processo. Essa verdade processual pode (ou não) corresponder à realidade histórica, sendo certo que é com base nela que o juiz deve proferir sua decisão.[112]

---

[110] REIS, Alexandre Cebrian Araújo e GONÇALVES, Victor Eduardo Rios. **Direito processual penal esquematizado**. Coordenador Pedro Lenza. – São Paulo : Saraiva, 2012. p. 247.
[111] Ob. Cit. p. 247
[109] LIMA, Renato Brasileiro de. **Manual de processo penal**, vol. l - Niterói, RJ: Impetus, 2011 .p.841.

Sendo certo que a lide será decidida com as provas trazidas aos autos, cabe as partes exaurirem todos os meios possíveis de produção de provas, a fim de demonstrar ao julgador a veracidade dos fatos alegados.

Dessa forma, entendida a busca da verdade processual, isto é, o juiz somente poderá decidir a questão, com as provas trazidas aos autos, sendo de fundamental importância que tanto a acusação como a defesa demonstre, através das provas, como efetivamente se deu o fato que motivou a investigação policial, a qual deu ensejo á ação penal.

3.4 Dos meios de Prova

Para que as partes provem os fatos alegados, podem utilizar de todos os meios de provas admitidos em nosso ordenamento jurídico e, embora exista um rol de possíveis meios de prova, este não tem caráter taxativo, não sendo forçoso reconhecer uma aplicabilidade subsidiária do art. 332 do Código de Processo Civil[113], aos meios de prova no processo penal

Em que pese nosso Código Penal enumerar alguns meios probatórios, dentre eles: exame de corpo de delito e outras perícias; o interrogatório do acusado; a confissão; as declarações do ofendido; as testemunhas; o reconhecimento de pessoas ou coisas; a acareação; os documentos; os indícios e a busca e apreensão, certo é que tal relação não é taxativa, ou seja, não exaure todas as possibilidades de meios de prova admitidos em nosso ordenamento, ou seja, tal rol é meramente exemplificativo.[114]

Ainda, os meios dizem respeito à forma pela qual se provará o alegado, isto é, trata-se de algo ulterior ao acontecimento dos fatos, de forma que quando exista mais de uma forma, ou seja, mais de um meio de demonstrar a veracidade dos fatos, poderão as partes se valer de todos aqueles que a lei não proíbe, ou optar por aquele que lhe seja mais conveniente.

> Dizem respeito, portanto, a uma atividade endoprocessual que se desenvolve perante o juiz, com o conhecimento e a participação das partes, cujo objetivo precípuo é a fixação de dados probatórios no processo. Enquanto as fontes de prova são anteriores ao processo e extraprocessuais, os meios de prova somente existem no processo.[115]

---

[110]"Art. 332. Todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, são hábeis para provar a verdade dos fatos, em que se funda a ação ou a defesa"

[114] REIS, Alexandre Cebrian Araújo e GONÇALVES, Victor Eduardo Rios. **Direito processual penal esquematizado**. Coordenador Pedro Lenza. – São Paulo : Saraiva, 2012. p. 256.

[115] AVENA, Norberto Cláudio Pâncaro. **Processo penal: esquematizado I**. 3 ed. - Rio de Janeiro: Forense; São Paulo: METODO, 2011. p.842.

Desse modo, caberá à parte buscar a melhor forma de comprovar suas afirmações, utilizando-se dos meios previstos no diploma legal, bem como de outros não expressamente previstos

Dentre os meios de provas não expressamente previstos, ou meios inominados, exemplificam-se filmagens, gravações de áudio, as fotografias e a inspeção judicial. O critério de admissibilidade dos meios de prova é estabelecido por exclusão, de forma que, tudo aquilo que, direta ou indiretamente, possa servir para formar o convencimento do magistrado acerca de como se deu o fato, é aceito como meio de prova. Este modelo de liberdade de prova, encontra seus limites na Constituição Federal, pelo princípio de vedação da prova ilícita.[116]

A Constituição Federal de 1988, assevera em seu art. 5ª, inciso LVI, que "são inadmissíveis, no processo, as provas obtidas por meio ilícito".

Deste modo, as provas obtidas por meio que não seja lícito, não podem integrar o processo, conforme determina o preceito constitucional. Como ilícita, entende-se aquela prova obtida através da violação de um direito, como por exemplo, a inviolabilidade do domicilio, estampado no art. 5º, inciso XI, da Constituição da República[117], que proíbe a violação do domicilio, salvo nos casos previstos na mesma norma.

No caso de a prova ter sido produzida através da violação do domicilio, sem o necessário consentimento do réu, será inadmissível em juízo, devendo ser desentranhada, a menos que seja o único meio de o réu provar sua inocência ou fato essencial à sua defesa, conforme ver-se-á adiante.

Assim, por certo, o legislador optou por não autorizar a admissão de provas obtidas por meio ilícito, para garantir a ordem e a segurança, uma vez que, caso fosse possível valer-se de qualquer meio para provar o alegado, as partes incorreriam na prática de desrespeito de outros direitos e garantias, abarcados pela Constituição como fundamentais.

Corroborando com o constante na Carta Magna de 1988, ao que se refere às provas ilícitas, é o Código de Processo Penal que adotou a teoria dos frutos da árvore envenenada, trazendo limites as provas, de forma a demonstrar quando são lícitas ou não, quanto a isso, doutrina Fernando Capez:

> (...) em face de sedimentado entendimento doutrinário e jurisprudencial, o art. 157 do CPP albergou a teoria dos frutos da árvore envenenada e trouxe limites a ela, inspirando-se na legislação norte-americana, de forma a se saber quando uma prova é

---

[116] REIS, Alexandre Cebrian Araújo; GONÇALVES, Victor Eduardo Rios. **Direito processual penal esquematizado**. Coordenador Pedro Lenza. – São Paulo : Saraiva, 2012. p. 256.

[117] "XI – a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;"

> ou não derivada da ilícita, isto é, a lei procurou trazer contornos para o estabelecimento do nexo causal entre uma prova e outra.[118]

Trazendo em seu art. 157[119], determinação expressa para que seja desentranhada dos autos a prova ilícita, obtida em violação as normas constitucionais ou legais, devendo ser admitidas em juízo, somente provas que não foram obtidas por intermédio de violação de direitos e garantias fundamentais, ainda que de forma indireta. Todavia, considerando o princípio *in dúbio pro reo*, mesmo em caso de a prova obtida por meio ilícito, há que se por na balança a liberdade do indivíduo e o outro direito ferido, como é o caso da inviolabilidade, cabendo ao intérprete do direito realizar o sopesamento no caso concreto, nesse sentido, é a lição de Norberto Cláudio Pâncaro Avena.

> Compreendemos assim que somente poderá instruir o processo aquela prova cuja procedência seja legal, isto é, que esteja dentro dos limites da lei, que não viole qualquer despeito da vedação constitucionalmente determinada, a jurisprudência majoritária desde muito tempo vem considerando possível a utilização das provas ilícitas em favor do réu, quando se trate da única forma de absolvê-lo ou, então, de comprovar um fato importante á sua defesa. Aplica, para tanto, o princípio da proporcionalidade, também chamado de princípio do sopesamento, o qual, partindo da consideração de que nenhum direito reconhecido na Constituição pode revestir-se de caráter absoluto, possibilita que se analise, na hipótese de colisão de direitos Fundamentais, qual deve, efetivamente, ser protegido pelo Estado. Destarte, sob a ótica dos interesses do acusado, imagine-se a hipótese em que, por melo de uma interceptação telefônica clandestina realizada sem ordem judicial, venha a ser descoberta a única prova capaz de inocentar o imputado da acusação que lhe foi feita. Neste caso, de um lado haverá a garantia constitucional da intimidade, violada com a interceptação realizada á revelia dos critérios legais; de outro, a garantia constitucional á liberdade, que restaria afrontada com uma condenação injusta. Ora, sopesando-se uma e outra garantia e havendo a prevalência da liberdade sobre a intimidade, impõe-se, nesta linha de pensamento, a admissão, em prol do réu, da prova ilicitamente obtida.[120]

Considerando o texto acima e trazendo para o cerne da presente pesquisa, levando em conta um crime cometido no âmbito virtual, cuja única forma do réu provar sua inocência ou demonstrar fatos importantes para sua defesa, seja através de uma prova obtida por meio ilícito, como por exemplo, através da invasão, não autorizada e sem ordem judicial, da caixa de e-mail de determinada pessoa, nesse caso, estar-se-á diante da afronta ao princípio constitucional

---

[118] CAPEZ, Fernando. **Curso de direito penal: legislação penal especial**, volume 4 – 7. ed. – São Paulo : Saraiva, 2012.p. 595.

[119] **Art. 157**. São inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais. § 1º São também inadmissíveis as provas derivadas das ilícitas, salvo quando não evidenciado o nexo de causalidade entre umas e outras, ou quando as derivadas puderem ser obtidas por uma fonte independente das primeiras. § 2º Considera -se fonte independente aquela que por si só, seguindo os trâmites típicos e de praxe, próprios da investigação ou instrução criminal, seria capaz de conduzir ao fato objeto da prova. § 3º Preclusa a decisão de desentranhamento da prova declarada inadmissível, esta será inutilizada por decisão judicial, facultado às partes acompanhar o incidente.

[120] AVENA, Norberto Cláudio Pâncaro. **Processo penal: esquematizado I**. 3 ed. - Rio de Janeiro: Forense; São Paulo: METODO, 2011. p.29.

previsto no art. 5º, inciso XII[121], que proíbe, dentre outros, a violação do sigilo das correspondências, das comunicações e de dados.

No caso descrito, haveria um conflito de garantias constitucionais, tendo em vista que a liberdade também se encontra prevista como uma das garantias fundamentais, grafada no *caput* do art. 5º da Constituição Federal[122], que, nos termos do texto constitucional, assegura a igualdade e a inviolabilidade do direito à vida e a **liberdade**.

No caso concreto, caberia ao legislador fazer a análise dos preceitos constitucionais, pautado, principalmente, na garantia da liberdade e no princípio *in dúbio pro reo*, decidindo, dessa forma, pela admissibilidade da prova produzida por meio ilícito, conforme tem sido o entendimento dos tribunais pátrios[123].

Ainda, em relação às provas ilícitas, conforme determina o art. 157 do Código de Processo Penal, cuja redação adveio da Lei n. 11.690/2008, as provas ilícitas devem ser desentranhadas, sendo assim entendidas aquelas obtidas com violação a preceitos constitucionais ou legais, bem como aquelas que lhe são derivadas. Todavia, poderá o magistrado, nos casos extraordinários, em que o único meio de provar a inocência do réu ou de demonstrar a veracidade de fato importante para sua defesa analisar este tipo de prova.

Ainda, no mesmo eixo temático, corroborando a afirmação de que as provas produzidas no ambiente virtual têm validade jurídica, importante frisar que o Código Civil

---

[121] "XI – 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 processual penal."

[122] "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:" (Grifou-se).

[123] RIO GRANDE DO SUL, Tribunal De Justiça de. "APELAÇÕES CRIMINAIS. RECURSOS MINISTERIAL E DEFENSIVO. TRÁFICO ILÍCITO DE DROGAS. PEDIDO DE MINISTERIAL DE EXASPERAÇÃO DA PENA. PEDIDO DEFENSIVO DE ABSOLVIÇÃO POR INSUFICIÊNCIA DE PROVA, DESCLASSIFICAÇÃO PARA O ARTIGO 28 DA LEI Nº 11.343/2006, RECONHECIMENTO DA FORMA PRIVILEGIADA, REDUÇÃO DA PENA E SUBSTITUIÇÃO DA PENA PRIVATIVA DE LIBERDADE POR RESTRITIVA DE DIREITOS. ILICITUDE DA PROVA MATERIAL Apreensão feita após invasão domiciliar não autorizada empreendida sem indicação da situação de flagrância, no pátio aos fundos da casa, sem que se tenha certeza quanto a ser o réu quem ali dispensou a droga, ele negando a posse. Insuficiência probatória que se resolve em favor do réu, com base no in dubio pro reo. Ilicitude da invasão reconhecida conforme precedente da Terceira Câmara Criminal: Apelação Crime Nº 70052586211, relator Des. Jayme Weingartner Neto, j. em 01/02/2013. RECURSO DEFENSIVO PROVIDO. RECURSO MINISTERIAL PREJUDICADO."(Apelação Crime Nº 70055009542, Terceira Câmara Criminal, Tribunal de Justiça do RS, Relator: João Batista Marques Tovo, Julgado em 19/09/2013). Disponível em: <http://www1.tjrs.jus.br/busca/?q=prova+il%EDcita+in+dubio&tb=jurisnova&partialfields=tribunal%3ATribunal%2520de%2520Justi%25C3%25A7a%2520do%2520RS.%28TipoDecisao%3Aac%25C3%25B3rd%25C3%25A3o%7CTipoDecisao%3Amonocr%25C3%25A1tica%7CTipoDecisao%3Anull%29&requiredfields=&as_q=>. Acesso em 03/10/2013, as 01h20min.

Brasileiro de 2002, inovou ao trazer em seu art. 225[124], a possibilidade de servirem como instrumento probatório, dentre outras, quaisquer reproduções mecânicas ou **eletrônicas**.

Cumpre esclarecer que tal dispositivo revela-se válido na esfera cível e embora o tema do presente trabalho seja voltado à área criminal, importante demonstrá-lo para firmar o entendimento de que o legislador tem aderido aos meios de prova da era digital.

3.5 Conceito de Persecução Criminal

Em relação à obtenção de provas, tanto na fase inquisitiva, quanto judicial, tem-se que, a primeira cabe à polícia judiciária civil, a qual atua investigando a materialidade, isto é, a existência do fato criminoso e autoria, a averiguação do possível autor do fato. Já a fase judicial, que é conduzida pelo magistrado, tem por objetivo analisar os fatos produzidos durante a investigação policial, bem como podem ser produzidas novas provas, como oitiva de testemunhas, juntada de documentos dentre outras, entendidas como pertinentes e não proibidas por lei.

Superadas essas duas etapas, tem-se o encerramento da instrução processual, devendo o juiz, através de todos os elementos levados aos autos, decidir, isto é, realizar o julgamento dos fatos e proferir uma sentença.

> (...) no aspecto relativo à polícia judiciária, cabe a condução das investigações necessárias, obtendo elementos de convicção e formando, com isso, o inquérito que servirá de supedâneo à instauração de uma futura ação penal. Ressalte-se que a conjugação dessa atividade investigatória realizada pela polícia judiciária com a ação penal deduzida pelo Ministério Público ou pelo ofendido constitui o que se chama de persecução penal. Enfim, trata-se esta de expressão que tem o significado de perseguir o crime visando à condenação e punição do infrator, traduzindo-se como atividade que envolve tanto a polícia Judiciária como quem detenha a legitimidade para instauração do processo criminal.[125]

Denomina-se persecução criminal a junção das duas fases (policial e judicial), incumbindo ao órgão competente, em cada uma delas realizar diligências para instruir o processo com as provas necessárias a fim de comprovar os fatos alegados.

---

[124] "**Art. 225**. As reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão."

[125] AVENA, Norberto Cláudio Pâncaro. **Processo penal: esquematizado I**. 3 ed. - Rio de Janeiro: Forense; São Paulo: METODO, 2011. p.164.

A incumbência de analisar todo o material probatório levado aos autos é do Poder Judiciário, que deverá, pautado naquilo que determina a lei, sentenciar o processo condenando ou absolvendo o réu, consoante tenha formado sua convicção.

> (...) é necessário que os órgãos estatais incumbidos da persecução penal obtenham provas da prática do crime e de sua autoria e que as demonstrem perante o Poder Judiciário, que, só ao final, poderá declarar o réu culpado e condená-lo a determinada espécie de pena.[126]

O deslinde do processo penal dependerá dessa forma de uma acusação formal, a qual deverá ser feita pelo titular do direito de ação, na grande maioria das vezes o Ministério Público, sendo que, após aceita a acusação, considera-se iniciada a ação penal. Durante esse trajeto entre o recebimento da acusação até a sentença final, devem ser observadas as regras processuais penais, que disciplinam o trâmite do processo, a essa sequência de atos é atribuído o nome de persecução criminal.

3.6 – Das peculiaridade da prova nos delitos informáticos

Embora nos delitos informáticos utiliza-se dos mesmos meios probatórios que nos demais crimes, há algumas peculiaridades, especialmente no que diz respeito à perícia técnica, feita por profissional especializado em informática. Tendo em vista a complexidade da linguagem computacional, necessário se faz o conhecimento técnico do perito que fará as constatações.

Desse modo, tem-se que por trás da facilidade de manusear um dispositivo informático, há programas complexos, com linguagens técnicas, as quais só podem ser decifradas por pessoas que detêm conhecimento necessário pra tal. O laudo do perito é de grande valia, servindo para fundamentação da decisão judicial.[127]

---

[126] REIS, Alexandre Cebrian Araújo e GONÇALVES, **Victor Eduardo Rios. Direito processual penal esquematizado**. Coordenador Pedro Lenza. – São Paulo : Saraiva, 2012. p.31.

[127]SÃO PAULO, Tribunal de Justiça de. "INDENIZAÇÃO. Violação de direitos autorais. Sentença de procedência. Perícia que concluiu pela utilização de programas de computador sem a regular licença. Laudo bem elaborado e analisado. Constatação de existência de 39 programas "piratas". Indenização em quantia equivalente a dez vezes o valor de um dos programas. Recursos desprovidos." (TJSP; EDcl 0001965-18.2010.8.26.0566/50000; Ac. 7001056; São Carlos; Quarta Câmara de Direito Privado; Rel. Des. Teixeira Leite; Julg. 20/06/2013; DJESP 18/09/2013). Disponível em: <https://www.magisteronline.com.br/mgstrnet/lpext.dll?f=templates&fn=main-hit-j.htm&2.0> Acesso em 07/10/2013, às 00h.

A perícia técnica tem por escopo descobrir o local de onde partiu o acesso criminoso, a data o horário, bem como o agente que cometeu o delito. Para chegar a tais informações, o perito deverá checar: os registros de *login* (*logs*)[128]; amostra de registros de sessão[129] e; registro de navegação na internet[130].

Após a checagem dos quesitos acima, quando possível encontrar o equipamento ou dispositivo informático de onde partiu ação criminosa, caso entenda necessário, os investigadores realizarão pedido ao poder judiciário para efetuar a busca e apreensão do equipamento, para colher possíveis provas que lá estejam armazenadas.

Todavia, não é simples a elucidação destes casos, especialmente quando o provedor de onde emanou o ato criminoso é estrangeiro e não possui escritório no Brasil.

Deste modo, torna-se difícil a investigação, principalmente para efetivar o pedido de informações ao provedor. No entanto, nesses casos é possível valer-se da ajuda de órgãos especializados, conforme explica Emerson Wented e Higor Vinicius Nogueira Jorge "Assim, no caso de e-mail, site ou conexão de internet ser de responsabilidade do provedor estrangeiro, deve-se contatar o Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI) do Ministério da Justiça."[131]

Assim, levando em conta a possibilidade do cometimento de crimes a partir de outros países, existe a possibilidade do pedido de informação ser feito a nação de onde agiu o agente

---

[128] WENTED, Emerson. JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação.** Rio de Janeiro: Brasport, 2012. "O log é o equivalente cibernético dos registros mantidos pela companhia telefônica, porém com uma leitura um pouco diferenciada, os *logs* são apresentados de uma forma mais bruta e desorganizada, sendo necessário um esforço maior para ser interpretado." p. 130.

[129] Registros que apresentam o nome do usuário, o endereço de IP designado, dia, data, horários de início e término, bem como duração da sessão. Ibidem. p. 130

[130] Ibidem . p. 131. "Toda vez que um usuário digita um endereço no seu navegador de internet ocorre o armazenamento de um registro, conforme já especificado. Portanto, o que pode ser encontrado pelo perito da coleta de evidências digitais corresponde a: *Diretório de cachê: cópias das páginas da web visitadas recentemente. * Arquivos de Histórico: lista de páginas visitadas recentemente ("CTRL + H"); Registros detalhados para cada pedido por qualquer página; Data, hora, número de bytes e, o mais importante, o endereço de IP do sistema que solicitou o dado."

[131] WENTED, Emerson. JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport, 2012. p. 131.

criminoso. O Brasil é signatário de um tratado de cooperação judicial (*Mutual Legal Assistence Treaty* - MLAT)[132], podendo o Brasil representar por essas medidas investigativas.[133]

Ainda, o Brasil faz parte de outra importante rede de assuntos voltados aos delitos informáticos, a *network for computer crime matter*[134], sendo que, em nosso país este órgão tem contato com o setor de crimes de informática da polícia federal.

Frise-se a importância da existência de tratados e acordos internacionais, para a troca de informações referentes aos crimes praticados no ambiente virtual, tendo em vista a possibilidade do agente cometer um crime contra a vítima que esteja a milhares de quilômetros de distância, em outro país, necessitando tão somente de um dispositivo com acesso a internet. Neste caso será solicitada ajuda do país de onde partiu a ação criminosa, para que diligencie no sentido de efetuar a colheita das informações que, em caso de demonstrarem a existência da materialidade e indícios da autoria servirão para integrarem a ação penal.

3.7 – Desafios na investigação dos crimes cibernéticos

Conforme já relatado ao longo da pesquisa, inúmeras são as dificuldades existentes para chegar-se ao agente ativo dos delitos informáticos, bem como para provar a ocorrência do

---

[132] Tratados assistência jurídica mútua (MLAT) permitem geralmente para a troca de provas e informações em matéria penal e relacionado. Em casos de lavagem de dinheiro, que pode ser extremamente útil como um meio de obtenção de serviços bancários e outros registros financeiros de nossos parceiros tratados. MLAT, que são negociados pelo Departamento de Estado, em cooperação com o Departamento de Justiça para facilitar a cooperação em matéria penal, em vigor com os seguintes países: Antígua e Barbuda, Argentina, Austrália, Áustria, Bahamas, Barbados, Bélgica, Belize , Brasil, Canadá, Chipre, República Checa, Dominica, Egito, Estônia, França, Alemanha, Grécia, Granada, Hong Kong, Hungria, Índia, Irlanda, Israel, Itália, Jamaica, Japão, Letônia, Liechtenstein, Lituânia, Luxemburgo, Malásia , México, Marrocos, o Reino dos Países Baixos (incluindo Aruba, Bonaire, Curaçao, Saba, St. Eustatius e St. Maarten), Nigéria, Panamá, Filipinas, Polônia, Romênia, Rússia, St. Lucia, St. Kitts & Nevis , St. Vincent & the Grenadines, África do Sul, Coreia do Sul, Espanha, Suécia, Suíça, Tailândia, Trinidad e Tobago, Turquia, Ucrânia, Reino Unido (incluindo a Ilha de Man, Ilhas Cayman, Anguilla, Ilhas Virgens Britânicas, Montserrat e Turks e Caicos), Uruguai e Venezuela. Disponível em <http://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm> Acesso em 06/10/2013.

[133] WENTED, Emerson. JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport, 2012. p. 132.

[134] "A Rede Hemisférica de Intercâmbio de Informações para a Assistência Mútua em Matéria Penal e Extradição (a "Rede") tem estado em desenvolvimento desde o ano de 2000, quando a Terceira Reunião de Ministros da Justiça ou de Ministros ou Procuradores-Gerais das Américas (REMJA-III) decidiu aumentar e melhorar a troca de informações entre os Estados membros da OEA na área da assistência mútua em matéria penal (...) O objetivo do sistema seguro de comunicação eletrônica é facilitar a troca de informações entre as autoridades centrais que lidam com questões de assistência mútua em matéria penal e extradição. Este sistema não só oferece um serviço seguro e-mail instantâneo às autoridades centrais, ele também oferece um espaço para reuniões virtuais e troca de documentos pertinentes." Disponível em < http://www.oas.org/juridico/mla/en/> Acesso em 06/10/2013>, às 23:30

fato e, com o crescente aumento do número de pessoas com acesso à internet, aumenta também o número de crimes deste gênero.

Os órgãos responsáveis pela persecução penal devem manter-se atualizados e constantemente realizarem treinamentos voltados aos crimes virtuais, de forma que saibam como proceder diante do caso concreto. Deve, dessa forma o Estado investir na capacitação dos agentes responsáveis pela apuração destes delitos, de forma que possam ser contundentes em diligenciar de forma eficaz para obtenção de provas.

Os *logs*, conforme já explicitado, é um dos meios de se chegar ao autor do delito, através da via judicial, será solicitado ao provedor de acesso a internet, o provedor de conteúdo, a *lan house*, ou ao administrador de rede privada, as informações relativas ao computador e o agente a quem foi atribuído o IP, conforme consta no *log.*

Grande dificuldade encontrada pelos responsáveis pela persecução criminal é o fato de que não há legislação que obrigue os usuários a preservarem os *logs* de acesso e conexão por um determinado prazo, o que, muitas vezes inviabiliza a comprovação da autoria do delito.[135]

Há ainda o problema da demora para realizar o efetivo cumprimento da ordem judicial, o que, pode levar a perda do material probatório, ou mesmo esse lapso possibilita que o agente destrua possíveis informações que levariam ao autor do delito.[136]

Outro problema, relaciona-se com a falta de legislação específica aos delitos informáticos, o que dificulta o enquadramento em uma norma tipificada, específica ao delito, sob pena de ferir o princípio constitucional previsto no art. 5º, inciso XXXIX da Constituição Federal, que estabelece: *nullum crimen nulla poena sine lege*[137].

Ainda, na ótica dos delegados de polícia civil Emerson Wented e Higor Vinícius Nogueira Jorge,[138] outro problema que atravanca a investigação policial é a necessidade de ordem judicial para obter toda e qualquer informação relativa a um *cybercrime*, representado excesso de burocracia, o que, prejudica ou retarda o esclarecimento dos delitos.

Outro fator que dificulta a persecução criminal nos delitos informáticos é a integração entre os delinquentes virtuais, que aproveitam-se dos meios de comunicação existentes na

---

[135] WENTED, Emerson. JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport, 2012. p. 177.
[136] Ibidem p. 177.
[137] "XXXIX – Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal."
[138]WENTED, Emerson. JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport, 2012. p. 180.

internet para planejarem, trocarem informações, tudo isso através de arquivos criptografados, de forma que somente o destinatário poderá ter acesso ao conteúdo enviado.[139]

Considerando as várias redes sociais existente, bem como os demais meios de comunicação *on-line*, tem-se que há grande facilidade para esse tipo de criminosos comunicarem-se, até porque estará resguardado o sigilo dos arquivos trocados, uma vez que estes podem ser criptografados, isto é, os arquivos, são "quebrados", desconfigurados, somente voltando ao formato original com a inserção de senha criada por quem o criptografou.

A criptografia e a estenografia, também são meios utilizados pelos criminosos para despistar os órgãos investigadores, de forma a tornar incompreensível a mensagem ou ocultá-la. A criptografia é um processo utilizado para misturar ou codificar dados ou informações, de forma a garantir que apenas o destinatário tenha acesso ao conteúdo.

Por outro lado, a estenografia permite esconder as informações no interior de outro arquivo, como um vídeo, texto ou áudio, sem que a pessoa que não tenha o conhecimento do arquivo oculto possa descobri-lo.[140]

O uso de *smartphones* também é apontado como fator que dificulta a investigação nestes crimes, tendo em vista que se trata de um aparelho móvel que está sempre junto ao seu proprietário, o que leva as pessoas a passarem mais tempo *on line*. Todavia, já existem programas maliciosos para esses equipamentos, os quais podem roubar dados dos usuários e até mesmo fazerem ligações não autorizadas.[141]

Os *smartphones* são celulares com acesso a internet, estão sempre a mão e, com a disseminação da internet, vários são os locais de acesso grátis à internet sem fio, bastando conectar o dispositivo e navegar, o que possibilita o agente utilizar vários provedores a partir de um mesmo aparelho eletrônico, fator que dificulta a persecução criminal.

Todavia, fator de determinante importância para os delitos informáticos, é o desconhecimento da vítima acerca dos riscos inerentes ao uso de equipamento informáticos.

> Grosso modo, pode-se dizer que os usuários de internet não conhecem a dimensão dos riscos que a utilização da rede mundial de computadores proporciona, nem as ameaças

---

[139] WENTED, Emerson. JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport, 2012. p. 181.
[140] Op. Cit. p. 182/183.
[141] CIRIAC, Douglas. Tecmundo.**Usuários reclamam de aplicativos com vírus na Android Market**. Usuários do Android foram surpreendidos por aplicativos mal-intencionados que baixaram do Android Market, a loja oficial de aplicativos para o sistema operacional portátil da Google. Os softwares maliciosos roubavam dados de usuários e até mesmo faziam ligações sem a autorização expressa do usuário. Disponível em <http://www.tecmundo.com.br/android/8959-usuarios-reclamam-de-aplicativos-com-virus-na-android-market.htm#ixzz2h0RB42cs > Acesso em 07/10/2013.

> que enfrenta ao receber um e-mail, acessar um site ou instalar um programa em seu computador.[142]

Com a popularização das redes sociais e o grande número de pessoas que tem aderido a elas, consequentemente torna-se alvo de pessoas com intenção de praticarem crimes na rede, considerando o grande número de pessoas desinformadas que não possuem conhecimento necessário para fugirem dos riscos da internet.

Quanto a esses riscos, podem ser prevenidos, através do aprendizado e da conscientização do perigo recorrente do uso da internet. É extremamente necessário agir com cautela, quando navega-se pela internet, observando os links, e-mails arquivos suspeitos, de forma a se precaver da ocorrência do delito.

Exemplo claro quanto aos desafios da investigação criminal nos delitos informáticos, é o caso "bolsa família", ocorrido em maio de 2013, no qual surgiram boatos que noticiavam o fim do referido benefício social, caso este, que foi arquivado por falta de provas, isto é ausência de autoria, bem como de suficiência de materialidade, conforme extrai-se de notícia veiculada pela imprensa do TJDFT (Tribunal de Justiça do Distrito Federal e dos Territórios).

> O MPDFT pediu o arquivamento do feito por não verificar "nenhuma comprovação idônea e adequada de que o crime em investigação tenha sido praticado e que a pessoa investigada, ou indicada pela vítima tenha agido com culpa ou mesmo dolo". O magistrado acolheu a manifestação ministerial para o arquivamento, considerando, no mesmo sentido, as conclusões obtidas pela investigação da Polícia Federal.O Juiz destaca em sua decisão o relatório final produzido pela delegada federal, no qual conclui pela "inexistência de elementos capazes de delimitar autoria e materialidade do suposto fato delitivo." Segundo a polícia, não seria possível identificar um ponto de origem das notícias anônimas vinculadas ao benefício bolsa família difundidas entre os dias 18 e 19 de maio de 2013.[143]

Com essas considerações, resta claro que, apesar de toda a tecnologia utilizada pela investigação, no presente caso a polícia federal, não foi possível apurar os indícios necessários para a propositura da ação penal, eis que ausentes a autoria e a materialidade.

Outro grande empecilho ao combate dos delitos informáticos é a "*deep web*", uma espécie de parte oculta, ou versão "underground" da internet, onde estão dados que não são encontrados na internet comum, isto é, através dos sites de busca conhecidos.

> Quando alguém quer navegar na internet, costuma recorrer a buscadores como o Google, Bing ou Ask. fm. Mas os dados que percorrem a rede mundial de computadores vão além do que é mostrado nessas ferramentas conhecidas como

---

[142] WENTED, Emerson. JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport, 2012. p. 184.

[143] Imprensa TJDFT. **Inquérito sobre boato do fim da bolsa família é arquivado.** Disponível em <http://www.tjdft.jus.br/institucional/imprensa/noticias/2013/julho/juiz-determina-arquivamento-de-investigacao-por-boato-do-fim-da-bolasa-familia> Acesso em 03/11/2013

> Crawlers (motores de busca). Muito do que não aparece nos resultados de busca, desde arquivos científicos, livros raros ou até mesmo novos vírus estão presente na "Deep Web" (Web Profunda).144

Na "*deep web*" pode-se encontrar o que há de pior na humanidade, desde assassinos de aluguel, venda de drogas e armas, até pedófilos e canibais, coisas que dificilmente consegue-se encontrar através da internet convencional.

> Há quem diga que o Google só consegue rastrear 1% do que existe online. Os outros 99% estariam na chamada Deep Web. Você já deve ter ouvido falar dela – e, se ouviu, provavelmente ficou em choque. Canibalismo e necrofilia são duas palavras comumente associadas à essa espécie de internet paralela, e servem como base para se ter uma noção do tipo de perversidade que se passa por lá.[145]

Embora, ainda, exista divergência quanto ao total anonimato daqueles que utilizam a "deep web", cumpre esclarecer que há casos em que houve a solução de crimes cometidos por meio desta versão da internet. Conforme notícia veiculada recentemente, pelo site Olhar Digital:

> Caiu nesta quarta-feira, 2, a Silk Road, um dos sites mais famosos da Deep Web, que comercializava drogas pela internet de forma semelhante ao eBay, utilizando a cripto-moeda BitCoin. O FBI conseguiu fechar o site e prender o chefe da operação, Ross Ulbricht, conhecido na rede profunda pelo pseudônimo Dread Pirate Roberts.[146]

Nota-se que grande parte dos usuários afirme que a impunidade é total, eis que não há como rastrear os acessos realizados na "internet underground", conforme visto, os crimes ocorridos neste meio podem ser solucionados a partir de outras linhas de investigação, que não o rastreamento do local do acesso.

Outrossim, importante frisar que recentemente a "*deep web*" tem ganhado maior número de adeptos, o que pode ser um problema, considerando o aumento do número de pessoas expostas a crimes, num campo de difícil investigação. Para que a internet não se torne um local "sem leis" se faz necessário a criação de uma ferramenta de controle, bem como uma regulamentação para o uso dessa internet "sem regras".

---

[144]PEDROSA, Leyberson**. Entenda o que é a Deep Web e saiba os riscos da navegação**. Portal EBC. Disponível em <http://www.ebc.com.br/tecnologia/2013/08/deep-web-riscos-e-usos-possiveis> Acesso em 10/11/2013.
[145]MELLO, João. Nem tudo são trevas: O lado bom da Deep Web. Revista Galileu. Disponível em <http://revistagalileu.globo.com/Revista/Common/0,,EMI331438-17770,00-NEM+TUDO+SAO+TREVAS+O+LADO+BOM+DA+DEEP+WEB.html> Acesso em 10/11/2013.
[146]Redação Olhar Digital. **FBI prende dono do maior site de venda de drogas da Deep Web**. Olhar Digital. Disponível em < http://olhardigital.uol.com.br/noticia/38012/38012> Acesso em 10/11/2013.

CONSIDERAÇÕES FINAIS

De todo o exposto, pode-se concluir que, em muito a evolução tecnológica contribuiu para melhoria da vida de todos, facilitando a comunicação em grandes distâncias, criando novas possibilidades para a medicina, comércio digital, dentre outras inúmeras vantagens advindas dessa era denominada Era da Informação.

De outro norte, junto com esse conforto e qualidade de vida, vieram também novos meios de cometer crimes, bem como novos crimes, os quais são praticados através de equipamentos informáticos, na maior parte das vezes através da internet, onde as vítimas, comumente são pessoas mal instruídas para usarem um equipamento informático e devido à falta de conhecimento, acabam se tornando "presas fáceis" para aqueles que utilizam a internet com fim de cometer delitos.

O direito, visando a realizar sua função que é justiça, tem buscado acompanhar essa evolução, que, diga-se de passagem, caminha a passos largos, motivo pelo qual não é fácil acompanhar, tendo em vista a complexidade e a demora para que seja aprovado um projeto de Lei. Em contrapartida, os criminosos, a cada dia desenvolvem novas técnicas para realizarem seus intentos.

Devido ao fato de os delitos informáticos serem uma matéria relativamente nova, cercada de termos próprios, muitos deles complexos e que os usuários comuns não conhecem e, ainda, à velocidade com que ocorre a evolução e o surgimento de novas ferramentas, programas e aplicativos, surgindo a cada dia novas terminologias, torna complexo o exame de matéria dos crimes cibernéticos para o universo jurídico.

Ainda, a questão da nomenclatura correspondente ao agente ativo dos delitos informáticos que, por falta de conhecimento é utilizada de forma errônea, atribuindo-se o adjetivo de hacker à aquele que prática uma conduta criminosa, o que, segundo restou demonstrado não é correto.

Quanto aos delitos informáticos, constatou-se que podem ser divididos em duas grandes categorias, os próprios, que são aqueles cujo bem atingido é o sistema informático e os impróprios, que dizem respeito aqueles crimes cujo ambiente virtual é apenas o meio pelo qual o agente utilizou para praticar um delito que pode ser cometido de outra forma.

Por fim, no que concerne as provas, restou claro que a principal dificuldade dos responsáveis pela persecução criminal, é obtenção dos dados quando há necessidade de busca

e apreensão de um equipamento, devido a demora para se conseguir autorização judicial, bem como o fato da inviolabilidade do sigilo, que se não for observada a prova será ilícita.

Por outro lado, a principal dificuldade, encontra-se nos meios utilizados pelos agentes criminosos, que muitas vezes, encontram maneiras de burlar a real origem do acesso, dificultando os trabalhos da investigação. Por fim, ainda, há que se mencionar a questão da "*deep web*", um local onde se pode navegar sem deixar rastros, isso é, pode-se cometer crimes e permanecer no anonimato, eis que não há como averiguar os dados da conexão nessa versão "underground" da internet.

Com tais considerações, conclui-se que, para que a justiça desempenhe seu papel de forma satisfatória, deve acompanhar a tecnologia, bem como é necessário investimento em aquisição de tecnologia de ponta (hardware e software) e treinamento dos profissionais responsáveis pela persecução criminal. Além do que, criação de legislação específica que permita formas mais céleres de tutelar os delitos informáticas e, por fim, principalmente, realizar campanhas de conscientização, de forma a prevenir a ocorrência deste tipo de delito.

REFERÊNCIAS

_____A Rede Hemisférica de Intercâmbio de Informações para a Assistência Mútua em Matéria Penal e Extradição. Disponível em: <http://www.oas.org/juridico/mla/en/>. Acesso em 06/10/2013.

_____As Licenças, **Creative Crommons.** Disponível em <http://creativecommons.org.br/as-licencas/>, acesso em 28/04/2013.

ABRIL, Editora. **A Era do Computador, Ciência & Natureza**. ABRIL Livros: Rio de Janeiro, 2010.

AVENA, Norberto Cláudio Pâncaro. **Processo penal: esquematizado I**. 3 ed. - Rio de Janeiro: Forense; São Paulo: METODO, 2011.

BONIS, Gabriel. **Carta Capital, Sociedade, Quase metade dos lares brasileiros já tem computadores**. Disponível em <http://www.cartacapital.com.br/sociedade/quase-metade-dos-lares-brasileiros-tem-computador/> acesso em 06/03/2013.

BRASIL, Base de dados portal do. **Historia Geral: Revolução Industrial**. Disponível em <http://www.portalbrasil.net/historiageral_revolucaoindustrial.htm>. acesso em 04/03/2013.

BRASIL. Presidência da República, Casa Civil, Subchefia para Assuntos Jurídicos. Lei nº 12.735, de 30 de novembro de 2012. Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm> Acesso em 18/04/2013.

CAPEZ, Fernando. **Curso de direito penal**: **legislação penal especial**, volume 4 – 7. ed. – São Paulo.

CAPEZ, Fernando. **Curso de direito penal**. Volume 1, parte geral: (arts. 1º a 120). 15. ed. — São Paulo: Saraiva, 2011.

CETIC.br. **Pesquisa TIC Domicílios 2010**. Disponível em :<http://www.cetic.br/usuarios/tic/2010/apresentacao-tic-domicilios-2010.pdf> Acesso em 19/04/2013.

CIRIAC, Douglas**.** Tecmundo.**Usuários reclamam de aplicativos com vírus na Android Market.** Disponível em <http://www.tecmundo.com.br/android/8959-usuarios-reclamam-de-aplicativos-com-virus-na-android-market.htm#ixzz2h0RB42cs > Acesso em 07/10/2013.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1 ed. 2ª tiragem, Saraiva: 2011: São Paulo.

Dicionário Aurélio Eletrônico de 2010.

Exame.com**. Número de brasileiros com acesso à Internet chega a 83 milhões.** Disponível em <http://exame.ABRIL.com.br/tecnologia/noticias/numero-de-brasileiros-com-acesso-a-internet-cresce-7> acesso em: 03/11/2013.

PANIZO, Francisco. NET ALMANAQUE. **Invenções que mudaram o mundo e sobreviveram ao tempo**. Disponível em: <http://www.superdicas.com.br/almanaque/almanaque.asp?u_action=display&u_log=254>. acesso em: 04 mar. 2013.

G1. Em São Paulo**. LEI 'CAROLINA DIECKMANN', que pune invasão de PCs, entra em vigor**, G1, Tecnologia e Games. Disponível em <http://g1.globo.com/tecnologia/noticia/2013/04/lei-carolina-dieckmann-que-pune-invasao-de-pcs-passa-valer-amanha.html> Acesso em 18/04/2013.

GONÇALVES, Victor Eduardo Rios. **Direito penal esquematizado: parte especial** – São Paulo : Saraiva, 2011.

GRANZOTTO, Claudio Geoffroy. **Análise da investigação preliminar de acordo com seus possíveis titulares**. Jus Navigandi. Disponível em: <http://jus.com.br/artigos/9522/analise-da-investigacao-preliminar-de-acordo-com-seus-possiveis-titulares#ixzz2gdGktOaC>.

GRECO, Rogério. **Código Penal: comentado** - 5. ed. - Niterói, RJ: Impetus, 2011.

IBOPE, Acesso à internet no Brasil atinge 94,2 milhões de pessoas. Disponível em: <http://www.ibope.com.br/pt-br/noticias/paginas/acesso-a-internet-no-brasil-atinge-94-milhoes-de-pessoas.aspx>. Acesso em: 06 mar. 2013.

Imprensa TJDFT. **INQUÉRITO SOBRE BOATO DO FIM DA BOLSA FAMÍLIA É ARQUIVADO.** Disponível em <http://www.tjdft.jus.br/institucional/imprensa/noticias/2013/julho/juiz-determina-arquivamento-de-investigacao-por-boato-do-fim-da-bolasa-familia>.

INELLAS, Gabriel Cesar Zaccaria de. **Crimes na Internet**. São Paulo: Editora Juarez de Oliveira, 2004.

KLEINA, Nilton. **A História da Internet: Pré-década de 60 até anos 80**. TECMUNDO, disponível em <http://www.tecmundo.com.br/infografico/9847-a-historia-da-internet-pre-decada-de-60-ate-anos-80-infografico-.htm>. acesso em 26/10/2013.

Lei 'Carolina Dieckmann. **Que pune invasão de PCs, entra em vigor**, G1, Tecnologia e Games. Disponível em <http://g1.globo.com/tecnologia/noticia/2013/04/lei-carolina-dieckmann-que-pune-invasao-de-pcs-passa-valer-amanha.html> acesso em 18/04/2013.

LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computacional**. 2ª ed. ATLAS S.A: São Paulo – 2011.

LIMA, Renato Brasileiro de. **Manual de processo penal**, vol. l - Niterói, RJ: Impetus, 2011.

MASSON, Cleber Rogério. **Direito penal esquematizado: parte especial I** - 3. ed. - Rio de Janeiro: Forense; São Paulo: MÉTODO, 2011. vol.2.

MELLO, João. Nem tudo são trevas: O lado bom da Deep Web. Revista Galileu. Disponível em: <http://revistagalileu.globo.com/Revista/Common/0,,EMI331438-17770,00-NEM+TUDO+SAO+TREVAS+O+LADO+BOM+DA+DEEP+WEB.html> Acesso em 10/11/2013.

MIRABETE, Julio Fabbrini. **Manual de Direito Penal**. Parte Geral Arts. 1º a 120 do CP Volume 1. 26 ed. rev. e atual. Editora Atlas S.A.: São Paulo. 2010.

MUOIO, Arlete Figueiredo. AGUIAR, Malu. **Crimes na Rede: O Perigo que se Esconde no Computador**. Companhia Ilimitada: São Paulo, 2006.

NEVES, Maria. **Falta de lei sobre crimes digitais leva à impunidade, diz especialista**. Agência Câmara de Notícias. Disponível em http://www2.camara.leg.br/camaranoticias/noticias/**CIENCIA-E-TECNOLOGIA/192143-FALTA-DE-LEI-SOBRE-CRIMES-DIGITAIS-LEVA-A-IMPUNIDADE,-DIZ-ESPECIALISTA**.html> acesso em 18/04/2013.

PEDROSA, Leyberson**. Entenda o que é a Deep Web e saiba os riscos da navegação**. Portal EBC. Disponível em <http://www.ebc.com.br/tecnologia/2013/08/deep-web-riscos-e-usos-possiveis> Acesso em 10/11/2013.

PEDROSO, Edson. **Termo Hacker, qual seu significado?**. Disponível em <http://www.oficinadanet.com.br/artigo/1476/termo_hacker_qual_seu_significado>. Acesso em 17 de ABRIL de 2013.

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

PRESIDÊNCIA, Da República, Casa Civil, Subchefia para Assuntos Jurídicos. **Lei nº 12.735**, de 30 de novembro de 2012. Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm> Acesso em 18/04/2013.

Redação Olhar Digital. **FBI prende dono do maior site de venda de drogas da Deep Web.** Olhar Digital. Disponível em < http://olhardigital.uol.com.br/noticia/38012/38012> Acesso em 10/11/2013.

REIS, Alexandre Cebrian Araújo e GONÇALVES, Victor Eduardo Rios. **Direito processual penal esquematizado**. Coordenador Pedro Lenza. – São Paulo : Saraiva, 2012.

RIO GRANDE DO SUL, Tribunal De Justiça. **Jurisprudência**. <http://www1.tjrs.jus.br/busca/?q=prova+il%EDcita+in+dubio&tb=jurisnova&partialfields=tribunal%3ATribunal%2520de%2520Justi%25C3%25A7a%2520do%2520RS.%28TipoDecisao%3Aac%25C3%25B3rd%25C3%25A3o%7CTipoDecisao%3Amonocr%25C3%25A1tica%7CTipoDecisao%3Anull%29&requiredfields=&as_q=>.

SÃO PAULO, Tribunal de Justiça de. **Jurisprudência**. Disponível em: < https://www.magisteronline.com.br/mgstrnet/lpext.dll?f=templates&fn=main-hit-j.htm&2.0> Saraiva, 2012.

Tratados assistência jurídica mútua (MLAT), disponível em: <http://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm>. acesso em 06/10/2013.

ZUFFO, João Antonio. **A Sociedade e a Economia no Novo Milênio: Os Empregos e as Empresas no Turbulento Alvorecer do Século XXI**. Livro I – A Tecnologia e a Infosociedade. São Paulo, Manole. 2003.

GLOSSÁRIO

Antivírus

Programa ou *software* especificamente desenvolvido para detectar, anular e eliminar de um computador vírus e outros tipos de código.

Arpanet

Acrônimo em inglês de Advanced Research Projects Agency Network (ARPANet) do Departamento de Defesa dos Estados Unidos da América, foi a primeira rede operacional de computadores à base de comutação de pacotes, e o precursor da Internet.

Autorreplicante

Tipo de vírus programado para criar cópias de si mesmo.

Cibernético

De cibernética - Ciência que estuda os mecanismos de comunicação e de controle nas máquinas e nos seres vivos.

Desktop

Termo da língua inglesa que designa o ambiente principal do computador. Literalmente, o termo tem o significado de "em cima da mesa". Era frequentemente utilizado para designar um computador de mesa por oposição ao laptop que é o computador portátil. Laptop tem o significado de "em cima do colo".

Firewall

Dispositivo constituído pela combinação de *software* e *hardware*, com objetivo de dividir e controlar o acesso entre redes de computadores.

Hardware

Parte física de um computador - Aquilo que se pode tocar em um dispositivo informático.

Ip

Ing.Sigla para Internet Protocol (Protocolo Internet). Padrão de endereçamento, por meio do qual um computador é identificado na Internet por um número exclusivo.

Lan house

Lan house é um estabelecimento comercial onde, à semelhança de um cyber café, as pessoas podem pagar para utilizar um computador com acesso à Internet e a uma rede local.

Microprocessador

É um circuito integrado que realiza as funções de cálculo e tomada de decisão de um computador. Todos os computadores e equipamentos eletrônicos baseiam-se nele para executar suas funções, podemos dizer que o processador é o cérebro do computador.

Programadores

De programador - desenvolvedor de software refere-se a alguém que faz programação de computadores e desenvolve software

Servidor

Sistema de computação centralizada que fornece serviços a uma rede de computadores.

Smartphone

Telefone inteligente, numa tradução livre do inglês - é um telemóvel com funcionalidades avançadas que podem ser estendidas por meio de programas executados por seu sistema operacional.

Software

Sequência de instruções escritas para serem interpretadas por um computador com o objetivo de executar tarefas específicas.

TCP/IP

Um conjunto de protocolos de comunicação entre computadores em rede ,(também chamado de pilha de protocolos TCP/IP). Seu nome vem de dois protocolos: o TCP (Transmission Control Protocol - Protocolo de Controle de Transmissão) e o IP (Internet Protocol - Protocolo de Interconexão).

Transações virtuais

Comércio eletrônico ou comercio virtual - é um tipo de transação comercial feita especialmente através de um equipamento eletrônico.

Vírus

Software malicioso que, tal como um vírus biológico, infecta o sistema.

World wide web

Rede de alcance mundial, também conhecida como Web ou WWW. World Wide Web é um sistema de documentos em hipermídia que são interligados e executados na Internet.