CENTRO DE PÓS GRADUAÇÃO, PESQUISA E EXTENSÃO

CRIMES DE INFORMÁTICA

Claudomiro Júnior de Castro Santos

Presidente Prudente/SP
2014

FACULDADES INTEGRADAS
"ANTÔNIO EUFRÁSIO DE TOLEDO"

CENTRO DE PÓS GRADUAÇÃO, PESQUISA E EXTENSÃO

CRIMES DE INFORMÁTICA

Claudomiro Júnior de Castro Santos

Monografia apresentada como requisito parcial de Conclusão de Curso para obtenção do título de Especialista em Direito Penal e Direito Processual Penal, sob a orientação do Prof.º Marcus Vinicius Feltrim Aquotti.

.

Presidente Prudente/SP
2014

CRIMES DE INFORMÁTICA

Monografia aprovada como requisito parcial para obtenção do título de Especialista em Direito Penal e Direito Processual Penal.

MARCUS VINICIUS FELTRIM AQUOTTI

EXAMINADOR 1

EXAMINADOR 2

Presidente Prudente, 07 de fevereiro de 2014.

DEDICATÓRIA

Primeiramente, a Deus, por me consentir um caminho iluminado e me proporcionar maravilhosos momentos de alegria, confiança, paciência, fidelidade, sabedoria e conhecimento.

À minha família, em especial meus pais, Claudomiro Izídio dos Santos e Maria Helena de Castro Santos, pelo amor e incentivo que me deram ao longo da minha vida e pela dedicação que tiveram para que eu alcançasse meus propósitos e por acreditarem no meu potencial, mesmo em meio a dificuldades.

Também dedico a minha irmã Bruna Izídio de Castro Santos e a minha namorada Suzane Ishibashi Moriki, por estarem ao meu lado, torcendo pela minha vitória.

“A adaptação é a grande lei da vida e do mundo não-vivo. São condições exteriores e interiores que tornam necessárias as adaptações, sem as quais não se estabeleceria um *modus vivendi* e desapareceriam os seres.”

Pontes de Miranda

AGRADECIMENTOS

Agradeço ao professor Marcus Vinicius Feltrim Aquotti pela atenção, dedicação, incentivo e ensinamentos, durante o período de orientação.

À dileta amiga Deborah Ramos da Silva pela ajuda com o *abstract* e as *keys*.

Por fim, agradeço a minha irmã Bruna Izídio de Castro Santos e a professora Daniela Martins Madrid, pelo auxílio na formatação do trabalho.

RESUMO

O presente trabalho acadêmico possui como tema a problemática que a Internet gerou para o ordenamento jurídico, por facilitar a violação ao direito à privacidade e a prática de delitos. O tema é de grande importância, uma vez que faz parte da nossa realidade, não tendo, porém, o devido tratamento doutrinário. A pesquisa foi baseada em livros, monografias e artigos, muitos fornecidos pela própria Internet. Primeiramente, o estudo tratou sobre a evolução histórica tanto dos computadores quanto da Rede das redes, apresentando algumas vantagens que a criação dela proporcionou para a humanidade, bem como seu lado negativo. Analisou algumas formas de invasão da privacidade alheia, e ainda trouxe conceitos sobre os hackers e crackers e também entrou na questão dos delitos informáticos. Sobre os delitos, o trabalho buscou conceituar e classificá-los, e alguns problemas que a prática deles através do sistema informático geram para os operadores do direito aplicarem a lei. Seguindo, o estudo tratou de alguns crimes de maior relevância, e ingressou na persecução criminal.

Palavras-Chave: Internet. Violação. Privacidade. Crimes de Informática. *Hackers. Crackers.*

ABSTRACT

The present academic work has as its theme a problematic about a Internet and their impacts on legal system, in order to facilitate understanding about the violation of the right to privacy and the practice of crime. The topic is of great importance, since it is part of our reality, however, it hasn't the proper doctrinal treatment. The research was based on books, monographs and articles many found with help on the Internet. Firstly, the study discusses about the historical evolution of both computers and the network. It presenting some advantages the creation this connectivity to humanity, as well as its down side. This job examine some forms of privacy concepts and give explanation about the hackers and crackers and the issue of computer crimes. On offenses, the study sought to conceptualize and classify them, and some problems who use the computer system generated for jurists apply the law. Subsequently, the study show a number_ of crimes of greater relevance, and demonstrate the criminal prosecution theirs.

Keys: Internet. Violation. Privacy. Computer Crimes. Hackers. Crackers.

SUMÁRIO

1 INTRODUÇÃO

Inicialmente criado para atender necessidades militares, o projeto que desenvolveu a Rede das redes tinha por objetivo apenas interligar os computadores das bases militares para garantir a integridade dos arquivos.

A evolução não parou e em pouco tempo ganhou novas funções, como a criação do e-mail que possibilitou o envio e recebimento de mensagens.

Com a criação do "WWW" as barreiras foram ultrapassadas. As possibilidades eram intermináveis, não existia distância a ser percorrida, o conceito de espaço geográfico não se aplicava à Rede, o mundo inteiro ao alcance das pessoas sem a necessidade de sair de casa.

Hoje é o meio de informação mais rápido que existe, atualizado em tempo real. No momento que alguém lança alguma informação na Rede, ela passa a estar disponível para pessoas de qualquer lugar do mundo acessarem.

O comércio também aproveitou a Rede, tanto para publicidade mais barata quanto para a criação de lojas virtuais, ou seja, venda pela Internet. A pessoa visita as páginas, olha os produtos e preços oferecidos e escolhe onde comprar e como pagar, como se estivesse em uma loja física.

Contudo, o mundo virtual não era perfeito. Com a popularização e inúmeras facilidades fornecidas aos usuários, tornou-se muito visado pelos criminosos, pois nele circulam grandes quantidades de dinheiro e informações.

Como ainda é um mundo em construção, criou-se a crença de que não havia regulamentação para as condutas praticadas nele, isso sem falar do anonimato e do despreparo inicial das autoridades, o que dificultava muito a identificação e punição dos agentes, fazendo com que a Rede das redes se tornasse um campo fértil para os criminosos.

Por estes fatores, o estudo do tema tornou-se relevante. É uma área ainda pouco explorada pela doutrina, que, no entanto, tem ganhado importância pelo significativo aumento na prática destes delitos nos últimos anos, forçando o Judiciário a se manifestar sobre os casos inéditos e, por vezes, inusitados.

Com isso, surgiram diversas dúvidas, como, por exemplo, se o Direito existente seria suficiente para regular as situações criadas pela Internet ou se por

esta ter peculiaridades o Direito deveria ser devidamente reformado. E se o crime praticado no mundo digital é outro crime ou apenas o meio que difere do convencional.

É notório que a nova tecnologia trouxe um grande desafio para o envelhecido Direito, sendo que este não consegue acompanhar o ritmo de constantes mudanças que o sistema informático passa a cada dia, tendo-se em vista o grau de complexidade para criação e modificação de normas pelo Legislativo.

Para o desenvolvimento do tema foi utilizado o método dedutivo, partindo do estudo da legislação vigente e da doutrina para então analisar casos em concreto.

Ainda foi utilizado o método dialético, contrapondo a tese de que o mundo virtual não possuía regras e a antítese de que era possível aplicar as normas vigentes, chegando a conclusão de que é possível se aplicar boa parte da legislação atual.

Como métodos auxiliares, foram utilizados o histórico e o comparativo, por meio dos quais foi realizado um estudo das origens do computador e da Internet, bem como a comparação entre os mecanismos de combate aos crimes comuns e aos praticados no mundo virtual.

A técnica de pesquisa utilizada foi a indireta bibliográfica, pois a pesquisa se baseou nos estudos feitos pelos juristas.

Primeiramente foi tratado da evolução histórica do computador e da Internet, bem com a relação desta com o Direito.

No capítulo seguinte foram abordadas as características da Internet e os meios de violação da intimidade e privacidade.

Por fim, foram estudadas as características dos crimes de informática, bem como alguns delitos de maior relevância e ainda a problemática do procedimento investigatório e da definição de competência.

2 EVOLUÇÃO HISTÓRICA

Para maior compreensão do presente estudo é preciso voltar no tempo e conhecer um pouco da história do computador e da Internet.

2.1 A Origem do Computador

Sua origem está muito distante dos dias atuais, há aproximadamente 2500 a.C., no Oriente Médio, era um quadro feito de barro com pedrinhas de calcário. Dois milênios mais tarde, os egípcios e os romanos utilizaram uma versão mais moderna, chamada de ábaco, para computar suas transações comerciais.

Em 1614, o escocês John Napier criou os Bastões de Napier e, com base nesse invento, o inglês Willian Oughtred criou o dispositivo chamado Cálculos de Proporção em 1633.

Por volta de 1822, Charles Babbage criou a Máquina das Diferenças, para o cálculo de tabelas e, em 1833, inventou a Máquina Analítica que poderia ser programada para diversas funções referentes a cálculos.

Com a II Guerra Mundial a necessidade de cálculos científicos aumentou e os computadores, que antes eram apenas mecânicos, passaram a ter componentes eletrônicos, iniciando a computação digital.

A evolução foi tamanha que ficou possível dividi-la em gerações:

> O computador ENIAC deu partida a uma série de gerações de computadores construídos com base em válvulas. Essa geração de máquinas sobreviveu entre os anos de 1946 até 1958. Assim, a *International Business Machine – IBM*, lança seu primeiro computador eletrônico, o *IBM 701*. A *Siemens*, na Alemanha, em 1958, lança o *Siemens* 2.002, enquanto a *IBM* nesse mesmo ano lança o *IBM 1.401.*
> A segunda geração de computadores caracterizava-se pelo uso de uma novidade tecnológica: os transistores. Cem vezes mais rápidos e confiáveis que as válvulas, os transistores desenvolvidos nos laboratórios *Bell* da *ATT* foram criados em 1948, passando a ser utilizados comercialmente no ano de 1959. Essa geração se desenvolveu entre os anos de 1959 e 1965, caracterizando-se pela redução surpreendente nas dimensões dos computadores, tornando-se mais confiáveis, mais rápidos e com menor consumo de energia. Foi na segunda geração que também surgiu o *software* e as primeiras linguagens de alto nível e também os primeiros sistemas operacionais. A terceira geração também advém de uma novidade

> tecnológica: os circuitos integrados inventados em 1958. Como a fabricação de circuitos integrados era uma tecnologia cara, sua utilização nos computadores só foi possível com o advento do programa espacial da NASA que, com suas necessidades específicas e encomendas maciças, viabilizou comercialmente a adoção dessa tecnologia. Essa técnica permitiu adotar numa minúscula pastilha (chip) de silício, inúmeros componentes eletrônicos, o que contribuiu para a sensível redução das dimensões dos computadores, favorecendo o aparecimento dos microcomputadores. Essa geração se desenvolveu até 1971. O que caracterizou a quarta geração dos computadores foi o avanço da fabricação de circuitos integrados (CIs). De início, surgiu a Integração em Larga Escala – (*Large Scale Integrato – LSI*), que conseguiu integrar alguns milhares de transistores em único chip. A fase seguinte, a quarta geração, (chamada *Very Large Scale Integratoery – VLSI*, em 1980), permitiu acondicionar centenas de milhares de transistores, após a qual seguiu-se o *ULSI*, que consegue reunir milhões de transistores em um único chip. Surgiram assim os supercomputadores e com eles as memórias (*Read and Memorize – RAM e Read Only Memory – ROM)*. (ROSA, 2002. p.26-27)

Com o passar do tempo as funções desempenhadas pelos computadores só aumentaram, sendo quase que ilimitadas e em contrapartida as dimensões apenas diminuíram, existindo atualmente os computadores de bolso, celulares e *tablets* com superprocessadores e sistemas operacionais.

Mas as necessidades militares deram origem à outra tecnologia tão importante quanto a anteriormente explanada, a Internet.

2.2 A Origem da Internet[1]

A compreensão da importância revolucionária da Rede mundial de computadores carece de uma digressão histórica sobre a Internet.

O projeto surgiu durante o período da Guerra Fria, na disputa de poder entre os EUA e a URSS. Quando a URSS lançou o satélite chamado "*Sputnik*", os EUA ficaram incomodados.

Após este evento os americanos, pensando num possível ataque nuclear, desenvolveram um meio de interligar os computadores das bases para que se uma delas fosse destruída a informação pudesse continuar a trafegar intacta. A ideia era um sistema descentralizado que mesmo destruído parcialmente

[1] Todos os parágrafos utilizados nesta seção secundária foram retirados do artigo Direito à Privacidade no Âmbito da Internet – Aspectos Civis e Penais, de minha coautoria, apresentado no V encontro de Iniciação Científica, IV Encontro de Extensão Universitária e I Encontro de Iniciação Científica para o Ensino Médio, Vol. 5, Nº. 5 (2009), ISSN 21-76-8498, publicado na Revista Eletrônica Intertemas.

permaneceria ativo continuando o tráfego das informações. Batizaram-na de Arpanet.

Posteriormente, “nos anos 70, a Internet passou a ser utilizada para fins acadêmicos e científicos” (CARDOSO, 2008, p.14).

A Rede cresceu tanto que a *Arpanet* não estava conseguindo controlar o tráfego digital, por isso foi criado um novo sistema para substituir o NCP, chamado de TCP/IP (*Transmission Control Protocol/Internet Protocol*).

Segundo explica Marcelo Cardoso (2006, p. 42-43):

> [...] o protocolo TCP é o encarregado de fragmentar, numerar, transportar e supervisar o processo de envio das informações através da Internet. Pois bem, o protocolo TCP não sabe a qual computador enviar as informações. Aqui entra em cena o protocolo IP. A função desse protocolo é justamente estabelecer os ‘endereços’ de origem e de destino de cada uma das partes (pacotes) de informação também é responsável pela escolha do ‘caminho’ que deve seguir cada transferência de informações através da Internet. [...]

As empresas foram autorizadas a ingressar na Rede somente em meados da década de 80. Posteriormente a Internet foi liberada ao público. Hoje as possibilidades são infinitas, o mundo todo está ligado a ela, que se tornou o maior (e mais rápido) veiculo de informação existente.

2.3 A Internet e o Direito

Com a popularização desses novos meios tecnológicos, a presença deles na vida das pessoas aumentou, sendo, inclusive, muito aproveitados pelos operadores do Direito que se utilizam da Internet para acompanhar a movimentação processual para maior celeridade dos atos processuais e, vivenciam outro avanço com a digitalização dos processos judiciais.

E contrapartida, este invento teve um lado negativo, porque contribuiu muito para a prática de delitos, pois a facilidade encontrada é maior.

Tendo em vista que o ciberespaço seria como outro mundo, é preciso de regras para que seja um bom lugar, por isso vem sendo comparado ao velho oeste americano do século XIX, pois é visto por alguns como um refúgio para os “foras-da-lei”, partindo do pressuposto de que as leis do mundo real não alcançariam esses criminosos atuantes no mundo virtual.

Era impossível para o legislador prever as novas situações geradas com a evolução tecnológica e ainda a velocidade em que ocorreu foi tamanha que mesmo com algumas atualizações, o ordenamento jurídico não conseguiu acompanhar tais mudanças.

Isso fez com que surgissem questionamentos sobre a eficácia do atual ordenamento jurídico frente à nova realidade, bem como se o melhor a se fazer seria atualizar as normas existentes ou se apenas a criação de uma legislação específica resolveria, o quem tem dificultado a abordagem jurídica do tema.

3 MECANISMOS DE VIOLAÇÃO DA INTIMIDADE E DA PRIVACIDADE POR MEIO DA INTERNET

Antes de falar sobre a Internet e os benefícios e riscos trazidos para a vida das pessoas com sua popularização, é preciso conceituá-la.

Conforme explica Aurélio (1999, p.1.126), Internet é:

> Qualquer conjunto de redes de computadores ligados entre si por roteadores e gateways, como por exemplo, aquela de âmbito mundial, descentralizada e de acesso público, cujos principais serviços oferecidos são o correio eletrônico, o chat e a web, e que é constituída por um conjunto de rede de computadores interconectados por roteadores que utilizam o protocolo de transmissão.

Atualmente a Internet possui muitas ferramentas que trazem comodidade a vida de seus usuários.

Segundo Marcelo Cardoso (2003, p.54):

> [...] a web é uma tecnologia que possibilita o acesso a documentos de hipertexto, vale dizer, páginas web, para recuperar informações nos servidores web.

Em breves palavras, o *e-mail* é uma ferramenta de envio e recebimento de mensagens. Com o advento da Rede das redes seu uso ficou mais prático, pois é possível abri-lo diretamente de uma página eletrônica em qualquer lugar.

Explica Marcelo Cardoso (2003, p. 63) que:

> O correio eletrônico caracteriza-se por ser um meio de comunicação rápido, barato, cômodo e relativamente fácil de utilizar, e que permite o intercâmbio de mensagens eletrônicas através da Internet.

Para utilizá-lo é necessário criar uma conta em um provedor que forneça o serviço de *e-mail*.

Outro interessante instrumento disponibilizado na Internet é a rede social. Hoje a mais famosa é o *Facebook*. Por meio das redes sociais é possível conversar com os amigos, conhecer pessoas do mundo todo, compartilhar pensamentos, fotos e vídeos, etc.

Como é possível acessar a Internet por meio de celulares e *tablets* as fotos e vídeos podem sem compartilhadas no momento em que são produzidas.

O modo de estudar também foi inovado pela Rede das redes. As instituições de ensino têm usado o ambiente virtual para complementar o aprendizado.

Por meio de páginas virtuais, tais instituições disponibilizam materiais de apoio, aulas *online* e ainda é possível a comunicação direta dos alunos com os professores para solução de dúvidas.

E, como esperado, nem o comércio ficou de fora da evolução trazida pela Internet:

> A Internet pode ser considerada uma ferramenta de aproximação entre as pessoas físicas e jurídicas. E o empresário, que sempre buscou transpor obstáculos para levar seus produtos e serviços a quem deles precisem, seja por terra, por água ou pelo ar, vê, agora, nos meios eletrônicos, um instrumento potencial – de custo relativamente baixo de suas 'especiarias'. [...]
> O comércio que, nos seus primórdios, foi desenvolvido por meio de feiras, de caravanas terrestres ou marítimas etc., chegou, ao final do século XX, impulsionado, ainda mais, por um sistema eletrônico que é a Internet, formando, então, o que se tem chamado de 'comércio eletrônico' ou *e-commerce.* (TEIXEIRA, 2013, p.127-128)

Hoje é possível fazer pesquisa de preços, comprar diversos produtos e até contratar serviços sem a necessidade de se deslocar fisicamente, bastando entrar, por meio de um aparelho eletrônico conectado à Internet, no endereço virtual da empresa desejada.

3.1 Intimidade e Privacidade

Com a popularização da Internet o acesso à informação ficou muito fácil, inclusive quanto as informações de outras pessoas.

Embora assegurado o acesso à informação pela Constituição Federal, é preciso verificar até que ponto os dados expostos em todo o ambiente virtual não ferem os direitos do cidadão.

Para isso é necessário saber o que é intimidade e vida privada, que também são direitos protegidos pela Carta Magna.

Conforme explica Alexandre de Morais (2007, p. 48):

> Os conceitos constitucionais de intimidade e vida privada apresentam grande interligação, podendo, porém, ser diferenciados por meio da menor amplitude do primeiro, que encontra-se no âmbito de incidência do segundo. Assim, intimidade relaciona-se às relações subjetivas e de trato íntimo da pessoa, suas relações familiares e de amizade, enquanto vida privada envolve todos os demais relacionamentos humanos, inclusive os objetivos, tais como relações comerciais, de trabalho, de estudo etc.
> Encontra-se em clara e ostensiva contradição com o fundamento constitucional da dignidade da pessoa humana (CF, art. 1º, III), com o direito à honra, à intimidade e à vida privada (CF, art. 5º, X) converter em instrumento de diversão ou entretenimento assuntos de natureza tão íntima quanto falecimentos, padecimentos ou quaisquer desgraças alheias, que não demonstrem nenhuma finalidade pública e caráter jornalístico em sua divulgação. Assim, não existe qualquer dúvida de que a divulgação de fotos, imagens ou notícias apelativas, injuriosas, desnecessárias para a informação objetiva e de interesse público (CF, art. 5º, XIV), que acarretem injustificado dano à dignidade humana autoriza a ocorrência de indenização por danos materiais e morais, além do respectivo direito à resposta.
> No restrito âmbito familiar, os direitos à intimidade e vida privada devem ser interpretados de uma forma mais ampla, levando-se em conta as delicadas, sentimentais e importantes relações familiares, devendo haver maior cuidado em qualquer intromissão externa. Dessa forma, concluímos como Antonio Magalhães, no sentido de que “as intromissões na vida familiar não se justificam pelo interesse de obtenção de prova, pois, da mesma forma do que sucede em relação aos segredos profissionais, deve ser igualmente reconhecida a função social de uma vivência conjugal e familiar à margem de restrições e intromissões”.
> Por outro lado, essa proteção constitucional em relação àqueles que exercem atividade política ou ainda em relação aos artistas em geral deve ser interpretada de uma forma mais restrita, havendo necessidade de uma maior tolerância ao se interpretar o ferimento das inviolabilidades à honra, à intimidade, à vida privada e à imagem, pois os primeiros estão sujeitos a uma forma especial de fiscalização pelo povo e pela mídia, enquanto o próprio exercício da atividade profissional dos segundos exige maior e constante exposição à mídia. Essa necessidade de interpretação mais restrita, porém, não afasta a proteção constitucional contra ofensas desarrazoadas, desproporcionais e, principalmente, sem qualquer nexo causal com a atividade profissional realizada.

Assim, verifica-se que há limites quanto à exposição de dados pessoais no mundo virtual e ainda que ultrapassar tais limites pode implicar em responsabilização do autor e de acordo com a gravidade do ato praticado, pode gerar desde indenização, até mesmo uma sanção criminal.

3.2 Mecanismos de Violação da Intimidade e da Privacidade

Como dito anteriormente, a finalidade inicial da Rede das redes era manter a ligação dos computadores e a circulação de dados, mesmo que parte dela fosse destruída.

Com isso, pouco foi pensado sobre a segurança desses dados, até porque o uso era exclusivo dos militares.

Contudo, com a abertura da Internet ao público a despreocupação com a segurança começou a gerar consequências negativas.

Marcelo Cardoso (2006, p. 164) explica que:

> Quando um usuário se conecta à Internet e começa a 'locomover-se' por ela, vai deixando muitos 'rastros' (dados e informações, de caráter pessoal ou não) por onde passa (página *web*, *mailing list*, grupo de *NEWS* etcs.).

Usuários com conhecimento avançado podem ter acesso a esses rastros ocasionando a violação da privacidade.

Alguns exemplos bem conhecidos de meios utilizados para invasão da privacidade são os *spams, trojans, cookies, spywares*, entre outros.

Para Fabrízio (2002, p. 65) *spam* é:

> O envio, de forma sistemática, indevida e imprópria, de mensagens não solicitadas, por correio eletrônico, que possam causar, de alguma forma, dano ou prejuízo a outrem.

Esta prática é muito comum por conta do uso descuidado do *e-mail* pelas pessoas. O alto número de e-mails que trafegam diariamente torna a fiscalização praticamente impossível, pois a grande quantidade deixa o provedor tecnicamente incapacitado para realizar qualquer tipo de controle sobre a informação contida neles.

Para diminuir a proliferação dos *spams* é preciso que os usuários utilizem mais as ferramentas disponibilizadas pelos provedores de correio eletrônico, como a denúncia de *spam,* a ocultação de endereços eletrônicos quando for enviar ou repassar mensagens a diversos contatos, evitar os *e-mails* de correntes.

Segundo Guilherme Tomizawa (2008, p.89-90):

> *Trojans* ou Cavalos de Tróia são programas executáveis que transformam seu micro em terminal de Internet "aberto". Estes programas eliminam as proteções que impedem a transferência de informações, ou seja, abrem uma porta de comunicação (*backdoor*) não monitorada.

Por mais que as ferramentas de proteção do computador evoluam, sejam atualizadas, o melhor anti-vírus que se pode ter é um usuário bem informado, consciente, responsável, que se mantém afastado de "lugares" do mundo virtual que possam apresentar riscos a seus equipamentos eletrônicos.

Na explicação de Guilherme Tomizawa (2008, p. 99):

> Os cookies são considerados 'uma invasão invisível a olho nu'. Consistem em pequenos arquivos gravados pelo servidor no disco rígido do usuário, os quais armazenam informações sobre os hábitos do usuário, frequência de visitas a um determinado site, tipos de notícias que prefere, etc. A cada nova conexão na Internet, essas informações são transferidas para o servidor de acesso, o que possibilita a inclusão do usuário numa lista classificada de acordo com seus hábitos de consumo. Depois de classificadas, essas informações podem ser vendidas aos comerciantes que a utilizam em mala direta ofertando produtos e serviços compatíveis com os hábitos do usuário. Também podem ser capturados dados referentes a ideologia, religião, crença, saúde, origem racial, orientação sexual e vida sexual do cidadão, dados estes que podem causar sérios prejuízos, caso venham a cair em mãos inescrupulosas.

Como visto, os cookies são rastros deixados na Internet pelo usuário, contendo informações suficientes para que seja traçado um perfil. Uma forma de evitar este incomodo é desativá-lo no navegador.

Quanto aos *spywares*, explica Guilherme Tomizawa (2008, p. 101-102) que:

> [...] se diferenciam dos *cookies* pelo fato de serem instalados no computador através de um programa gratuito (*freeware*) ou um programa de uso limitado (*shareware*), o qual são oferecidos com a promessa de facilitar a vida do internauta. Porém, esse programa vem acompanhado de um *spyware*, um código que possibilita rastrear as informações do usuário. De posse dessas informações, pode-se oferecer uma série de produtos e traçar o perfil do internauta para outras empresas, caracterizando uma verdadeira

> violação de privacidade. Aos *spywares* segue-se, em consequência, o *spam*.

Outra forma de se obter dados dos internautas é a engenharia social, sendo a Internet só mais um meio de praticá-la.

Para Guilherme Tomizawa (2008, p. 102):

> [...] define-se engenharia social como o conjunto de técnicas usadas por invasores para convencer as pessoas a instalar programas maliciosos, divulgar informações confidenciais etc, ou seja, são técnicas que buscam explorar o usuário em um ponto frágil, a informação e o conhecimento.

O alvo é o usuário e o que se explora é a confiança da vítima, que é envolvida pela astúcia do autor e acaba caindo no golpe, fornecendo as informações solicitadas.

É muito comum se ver a atuação de engenheiros sociais por meio de *e-mails* em nome de órgãos governamentais ou de grandes empresas, com situações justificadoras da solicitação de dados, o que faz com que usuários menos informados sejam enganados.

Outro risco a privacidade é o comércio eletrônico. Por conta da necessidade de realizar cadastros dos clientes, formam banco de dados.

Com a criação dos cadastros, duas situações podem ocorrer: a possibilidade de invasões do sistema para obtenção de dados e a venda desses dados pela própria empresa na qual as informações foram prestadas.

Deve o internauta escolher com muito cuidado os comércios eletrônicos em que fará compras.

Por fim, resta ao internauta sempre se manter atualizado, pois mesmo os meios de violação baseados em programas maliciosos ainda contam com a desinformação do usuário que acaba, sem perceber, facilitando a invasão de computador ou outro eletrônico.

4 CONCEITO, CLASSIFICAÇÃO E SUJEITO ATIVO E PASSIVO DOS CRIMES DE INFORMÁTICA

Com a criação e difusão dos computadores e da Internet surgiu uma figura muito interessante, conhecida como *hacker.*

Conforme explica Marcelo Xavier (2011, p.95):

> *Hacker* é o nome genérico dado aos chamados "piratas" de computador. Essa expressão surgiu nos laboratórios de computação do *MIT* (*Massachusetts Institute of Technology*), onde estudantes passavam noites em claro averiguando tudo o que se podia fazer com um computador.
> A melhor tradução para referida expressão inglesa é "fuçador". Entretanto, muitas são as discussões sobre o real significado do citado termo.
> [...]
> A definição mais aceita é que *hacker* é qualquer um que tenha grande conhecimento sobre computadores e faça invasões.
> Apesar da fama de "criminosos virtuais", nem todo *hacker* deseja o prejuízo alheio.

Saber o básico não é suficiente para um *hacker*, ele precisa saber tudo que, por exemplo, um *software* é capaz de fazer.

São movidos pela curiosidade, pelo desejo por conhecimento, e essa vontade de saber mais e mais é o que os diferencia dos demais usuários, que se contentam com o que lhes é oferecido.

Por isso, muitas empresas acabam contratando-os para encontrarem os pontos vulneráveis de seus sistemas de segurança para que assim essas falhas na defesa possam ser corrigidas.

Contudo, nem todos os usuários que são "*expert em informática"*, usam suas habilidades em sistemas, programações, redes, etc... para melhorar a Rede das redes e ganharem mais conhecimento.

Alguns seguem outros caminhos, para satisfação própria, com a finalidade de causar danos a outros usuários ou empresas e assim obterem fama e dinheiro.

Como a palavra era usada de maneira generalizada pela imprensa, começou a incomodar os verdadeiros hackers que, para se defenderem, criaram o termo *"cracker"* para definir esse grupo de criminosos e assim diferenciá-los dos *"hackers éticos"*.:

> Eles se divertem com destruições de sites e sua repercussão na imprensa. São também ladrões, valendo-se da Internet para roubar dinheiro e informações.
> O *cracker* é aquele que, basicamente, "quebra" um sistema de segurança, invadindo-o. Fanáticos pelo vandalismo, também adoram "pichar" páginas

> da *web* deixando, na maioria das vezes, mensagens de conteúdo ofensivo e racista. (CRESPO, 2011, p.96)

Logo, é possível concluir que o verdadeiro *hacker* é movido por sua curiosidade, pela busca do conhecimento sobre o funcionamento de programas, sistemas, enquanto que o cracker visa apenas causar danos ou obter vantagem financeira, por meio de seus conhecimentos em informática.

Os alvos dos crackers geralmente são sites famosos, do governo, de empresas de segurança, empresas de telecomunicações, empresas de tecnologia e bancos.

As motivações de tais condutas são variadas, podendo ser um manifesto, um funcionário insatisfeito, busca por dinheiro, mera diversão ou apenas busca pela fama, dentre outras.

4.1 Conceito de Crime de Informática

São muitas as denominações utilizadas para se referir as condutas ilícitas praticadas no mundo virtual. Alguns exemplos são crimes de computador, crimes na Internet, cibercrimes, crimes digitais, crimes virtuais, crimes eletrônicos ou crimes de informática.

Quanto à sua conceituação, Carla Rodrigues (2003, p.09) entende que:

> Crime de informática é aquele praticado contra o sistema de informática ou através deste, compreendendo os crimes praticados contra o computador e seus acessórios e os perpetrados através do computador. Inclui-se neste conceito os delitos praticados através da Internet, pois pressuposto para acessar a rede é a utilização de um computador.

Deste modo, a melhor denominação seria crime de informática, por ser mais ampla que as demais, ou seja, não só os crimes praticados dentro da Rede, mas todos que envolvam o sistema de informática, considerando os crimes praticados por meio da Internet uma espécie.

4.2 Classificação dos Crimes de Informática

Quanto à classificação, é possível estabelecer uma divisão dos crimes de informática em próprios ou impróprios.

Para Carla Rodrigues (2003, p. 10):

> Os primeiros são aqueles que só podem ser praticados através da informática, sem ela é impossível a execução e consumação da infração. Na verdade os crimes de informática próprios surgiram com a evolução desta Ciência, são tipos novos, que agridem a informática como bem juridicamente protegido. Daí porque, em face da escassa legislação existente, alguns fatos são atípicos e, portanto, não podem ser punidos.

Como exemplo de crime de informática próprio é possível citar a violação de direito de autor de programa de computador prevista na Lei nº. 9.609/98, bem como a invasão de dispositivo informático e a interrupção ou perturbação de serviço informático ou telemático, recentemente tipificadas pela Lei nº. 12.737/12.

Em relação aos crimes de informática impróprios, explica Carla Rodrigues (2003, p. 10) que:

> [...] são os que podem ser praticados de qualquer forma, inclusive através da informática. Assim, o agente, para cometer o delito, utiliza, eventualmente, o sistema informático. O computador é um meio, um instrumento para a execução do crime. São delitos que violam bens já protegidos por nossa legislação, como o patrimônio, a honra etc. Exemplo: ameaça, estelionato, calúnia [...]

Feitas essas considerações sobre os delitos de informática, surgem algumas questões, como por exemplo: como punir aqueles que os praticam, se não há lei tipificando essas condutas? Seria possível aplicar as normas existentes no Direito Penal no que couber? E como ficaria o princípio da legalidade e o princípio da proibição da analogia *"in mallam partem"*?

A responsabilidade penal, por recair sobre direito constitucional do cidadão (*liberdade de locomoção*), deve ser aplicada de forma mais restrita, especialmente porque um dos princípios que regem o direito penal é o da legalidade, presente no artigo 5º, inciso XXXIX da Constituição Federal e no artigo 1º do Código Penal, afirmando que "não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal".

Nos crimes praticados através do sistema informático é possível afetar diversos bens jurídicos, muitos já tutelados pelo ordenamento penal, então seria possível enquadrá-los nos tipos penais já existentes.

Entretanto, conforme leciona Damásio (2009, p.09), há outro princípio fundamental que rege o Direito Penal, chamado de Princípio da Proibição da Analogia *"In Mallam Partem"*, extraído do princípio anteriormente citado, proibindo a adequação típica "por semelhança" entre fatos.

Com isso, havia divergência sobre como resolver essas questões. Por um lado utilizar as leis existentes na tentativa de evitar a impunidade, mas correndo o risco de ser questionada a validade dos atos praticados, sob a alegação de atentarem contra princípios fundamentais e ter todo o procedimento anulado ou então reconhecer a necessidade de leis específicas, aguardar a atualização do ordenamento jurídico e, por falta de previsão legal, conhecer a atipicidade das condutas.

Contudo, para evitar a impunidade, que geraria o aumento da prática desses atos por meio do sistema informático, os juízes passaram a enquadrar as condutas praticadas no mundo digital às leis existentes no mundo real.

Com o grande aumento do número de processos envolvendo casos de pratica de crimes virtuais, estes começaram a alcançar o Superior Tribunal de Justiça, que se posicionou da seguinte forma:

> A Internet ainda é tida por muitos como um território livre, sem lei e sem punição. Mas a realidade não é bem assim: diariamente, o Judiciário vem coibindo a sensação de impunidade que reina no ambiente virtual e combatendo a criminalidade cibernética com a aplicação do Código Penal, do Código Civil e de legislações específicas como a Lei n. 9.296 – que trata das interceptações de comunicação em sistemas de telefonia, informática e telemática – e a Lei n. 9.609 – que dispõe sobre a proteção da propriedade intelectual de programas de computador.
> Na ausência de uma legislação específica para crimes eletrônicos, os tribunais brasileiros estão enfrentando e punindo internautas, crakers e hackers que utilizam a rede mundial de computadores como instrumento para a prática de crimes. Grande parte dos magistrados, advogados e consultores jurídicos considera que cerca de 95% dos delitos cometidos eletronicamente já estão tipificados no Código Penal brasileiro por caracterizar crimes comuns praticados por meio da Internet. Os outros 5% para os quais faltaria enquadramento jurídico abrangem transgressões que só existem no mundo virtual, como a distribuição de vírus eletrônico, cavalos-de-tróia e worm (verme, em português).
> Para essa maioria, a Internet não é um campo novo de atuação, mas apenas um novo caminho para a realização de delitos já praticados no mundo real, bastando apenas que as leis sejam adaptadas para os crimes eletrônicos. E é isso que a Justiça vem fazendo. Adaptando e empregando vários dispositivos do Código Penal no combate ao crime digital. [...] O STJ, como guardião e uniformizador da legislação infraconstitucional, vem consolidando a aplicação desses dispositivos em diversos julgados. [...] Os casos de furto e estelionato virtual também já foram devidamente enquadrados pela Corte. (COORDENADORIA DE EDITORIA E IMPRENSA DO STJ, 2008, p.01)

Com o parecer favorável do Superior Tribunal de Justiça, a questão relativa aos crimes que se enquadram na legislação existente foi pacificada, restando apenas a dúvida sobre o que fazer nos casos em que se tratar de delitos puros, que não possuem previsão legal e que por força dos princípios fundamentais do Direito Penal são considerados atípicos.

O que se constata, assim, é que se faz urgente uma atualização legislativa tipificando as condutas delitivas puramente do sistema informático, para que o ordenamento jurídico possa se adequar a esta nova realidade virtual, propiciando a efetiva responsabilização penal dos infratores.

4.3 Sujeito Ativo e Passivo

O conceito de sujeito ativo e passivo dos crimes de informática é o mesmo existente para os crimes comuns.

Conforme leciona Damásio (2009, p.163), “sujeito ativo é quem pratica o fato descrito na norma penal incriminadora. Por ser o delito ação humana, indubitável que o sujeito ativo é o homem.” Logo, qualquer pessoa pode ser autora de um crime.

Todavia, há algumas denominações do sujeito ativo nos delitos virtuais de acordo com a infração penal cometida. *Crackers* seriam considerados gênero, demais qualificações seriam suas espécies.

Assim como no mundo real, onde há denominações diferentes para os diversos tipos de criminosos, como estelionatário, estuprador entre outros, no mundo virtual não é diferente, separando-se os infratores de acordo com as condutas praticadas.

Como exemplo, *warez* são aqueles que copiam softwares pagos e distribuem gratuitamente; *caders* são especialistas na falsificação de cartões de crédito, para utilização fraudulenta na rede; *insiders* geralmente são próximos as vítimas que pretendem prejudicar, como o caso de empregados insatisfeitos ou ex-empregados, que por terem conhecimento sobre o funcionamento da empresa, têm maior facilidade na ação.

Enfim, de acordo com as condutas de cada um dos ‘personagens’ mencionados, seria possível criar uma tipificação penal própria, que pudesse efetivamente combatê-los.

Já o sujeito passivo é “o titular do bem jurídico tutelado pela norma penal. Divide-se em sujeito passivo constante ou formal e sujeito passivo eventual ou material.” (GONÇALVES E ESTEFAM, 2012, p.184)

Olhando o delito sobre o aspecto formal, violando a norma penal há uma lesão ao bem tutelado por ela, pelo simples fato de ter praticado a conduta há um sujeito passivo formal, independente dos efeitos do crime, que é o Estado, titular do mandamento proibitivo.

Sobre o aspecto material, explicam André Estefam e Victor Eduardo (2012, p. 184) que:

> A vítima da infração, isto é, o titular do bem jurídico protegido na norma penal, por sua vez, considera-se sujeito passivo eventual ou material. Podem ser sujeitos passivos eventuais de crimes: o ser humano, desde a concepção, a pessoa jurídica, o Estado, a coletividade e até mesmo os entes sem personalidade jurídica.

Teoricamente qualquer um pode ser sujeito passivo de delitos virtuais, porém os infratores geralmente estão atrás de fama e fortuna, de modo que, direcionam os alvos a sites famosos, empresas de segurança, lojas virtuais, bancos.

A dificuldade no combate a esses delitos nem sempre é causada pela complexidade em se identificar a autoria, mas sim no silêncio das vítimas.

As empresas virtuais muitas vezes preferem arcar com os prejuízos causados a se exporem e mostrar sua vulnerabilidade, correndo o risco de novos ataques e de perderem seus clientes, tendo um prejuízo ainda maior.

Um banco, por exemplo, que teve seu sistema de segurança burlado e várias contas de clientes limpas, pode preferir devolver os valores às contas a noticiar o crime, pois a exposição poderia ocasionar novos ataques, sem falar na perda de clientes por não ser tão seguro quanto pensavam.

Isso não é regra, mas acontece por uma questão puramente matemática, na qual contabilizando os prejuízos e os riscos, optam pelo que for mais viável, o que muitas vezes significa deixar de informar sobre a ocorrência de um delito e, consequentemente, contribuir com a impunidade.

5 CRIMES EM ESPÉCIE

O presente capítulo versa sobre alguns dos crimes praticados no mundo virtual, que apresentam maior relevância, sendo alguns apenas potencializados pelo sistema informático, enquanto outros são condutas puramente do mundo virtual.

5.1 Crimes Contra a Honra

Previstos nos artigos 138 a 140 do Código Penal, são tipos penais criados para proteção da honra.

Explica Gustavo Octaviano (2011, p. 245) que a honra:

> Ainda que imaterial, é valor inerente á dignidade humana. Conjunto de atributos morais, físicos e intelectuais da pessoa, que lhe conferem autoestima e reputação. Quando tratamos da autoestima, falamos de honra subjetiva. A reputação está relacionada com a honra objetiva. A honra objetiva pode ser compreendida como o juízo que terceiros fazem acerca dos atributos de alguém. Honra subjetiva, o juízo que determinada pessoa faz acerca de seus próprios atributos.

O legislador dividiu em três tipos diferentes de se ofender a honra de alguém, que são: calúnia, difamação e injúria.

Ao ler o Código Penal brasileiro é possível extrair que caluniar é imputar falsamente a alguém fato que constitui crime e difamar é atribuir fato ofensivo à reputação de alguém.

Por tratarem da honra objetiva, para que haja consumação dos crimes de calúnia e difamação é preciso que chegue ao conhecimento de terceiros os fatos imputados a alguém. Caso somente a vítima tenha conhecimento, sua reputação não sofrerá dano.

Por fim, no tipo penal de injúria, como a pretensão é resguardar a integridade da honra subjetiva, não importa para sua consumação se terceiro teve ou não conhecimento das ofensas.

Aqui o autor não imputa a vítima um fato desonroso ou uma conduta criminosa, ele atribui uma característica negativa à imagem que o indivíduo tem de si, por isso pouco importa se foi realizada na presença ou se houve o conhecimento de terceiro.

Esses crimes costumam ocorrer no mundo virtual durante conversas instantâneas em salas de bate-papo, fóruns, sites de relacionamento, na criação de sites e no envio de e-mails. As ofensas poderão ocorrer através desses mecanismos de comunicação e a consumação dependerá da espécie do crime e de suas circunstâncias.

.

5.2 Furto

É considerado um crime de informática impróprio, por ser o sistema informático apenas mais um meio de praticá-lo. Há também a necessidade da coisa furtada ter valor econômico, para configuração do crime.

Conforme explica Capez (2013, p.352):

> Hoje em dia é muito comum a subtração de valores das instituições financeiras por intermédio do sistema de informática. Assim, com o avanço dos meios tecnológicos, os meios executórios do crime estão cada vez mais elaborados e ágeis, não havendo, muitas vezes, sequer a apreensão física da *res,* tal como ocorre com a transferência de numerários pela rede mundial de computadores. Nessa hipótese, reputa-se configurado o crime no momento em que os valores são transferidos para a conta do agente, não havendo que se discutir se há posse tranquila ou não da *res.*

Não se trata de estelionato, pois não há a entrega espontânea do bem pela vítima ao agente, mas sim a subtração do bem sem que a vítima perceba. E, ainda, a conduta é qualificada pelo uso de fraude.

Corroborando com o explanado, o Superior Tribunal de Justiça elucida em seu julgado que:

> [...] 1. O furto mediante fraude não se confunde com o estelionato. A distinção se faz primordialmente com a análise do elemento comum da fraude que, no furto, é utilizada pelo agente com o fim de burlar a vigilância da vítima que, desatenta, tem seu bem subtraído, sem que se aperceba; no estelionato, a fraude é usada como meio de obter o consentimento da vítima que, iludida, entrega voluntariamente o bem ao agente.

> 2. Hipótese em que o agente se valeu de fraude eletrônica para a retirada de mais de dois mil e quinhentos reais de conta bancária, por meio da "Internet Banking" da Caixa Econômica Federal, o que ocorreu, por certo, sem qualquer tipo de consentimento da vítima, o Banco. A fraude, de fato, foi usada para burlar o sistema de proteção e de vigilância do Banco sobre os valores mantidos sob sua guarda. Configuração do crime de furto qualificado por fraude, e não estelionato. [...] (SUPERIOR TRIBUNAL DE JUSTIÇA. CC 67343 / GO (CONFLITO DE COMPETENCIA 2006/0166153-0). Relatora Ministra LAURITA VAZ (1120) órgão julgador s3 - terceira seção, data do julgamento 28/03/2007, data da publicação/fonte dj 11/12/2007, p.170).

Assim, estaria pacificada a discussão sobre qual seria a melhor capitulação para o caso em tela, bem como demonstrado que os infratores não se isentarão da aplicação da lei.

5.3 Estelionato

O crime de estelionato, no ordenamento jurídico pátrio, é tipificado no artigo 171 do Código Penal.

Segundo explica Victor Eduardo (2013, p. 446):

> O estelionato é um crime marcado pelo emprego de fraude, uma vez que o agente, valendo-se de alguma artimanha, consegue enganar a vítima e convencê-la a entregar-lhe algum bem e, na sequência, locupleta-se ilicitamente com tal objeto.

O sistema informático é apenas mais um meio de praticar o referido delito. A ludibriação pode ocorrer através de salas de bate-papo, *sites* e *e-mails*.

Dispõe o artigo 171 do Código Penal que o meio utilizado pelo autor é ardil, artifício ou qualquer outro meio fraudulento. Segundo explica Victor Eduardo (2013, p.446 e 447):

> O artifício se mostra presente quando, para enganar a vítima, o agente lança mão de algum artefato, faz uso de algum objeto para ajudá-lo no engodo. [...]
> O ardil é a conversa enganosa, ou seja, o agente engana a vítima com mentiras verbais. [...]
> Por fim, a expressão qualquer outro meio fraudulento é uma fórmula genérica, inserida no tipo penal para abranger qualquer outra artimanha capaz de enganar a vítima, como, por exemplo, o silêncio. [...]

Com advento do comércio eletrônico, tornou-se mais fácil a prática de estelionato no mundo virtual, pois atualmente a utilização do mundo virtual para a prática das relações de consumo se popularizou.

Por isso, entende-se que a fraude ocorre quando o indivíduo normalmente comprando ou vendendo via Internet é enganado de alguma forma ou quando há descrição enganosa de produto ou serviço ou ainda pelo recebimento do pedido e dinheiro, sem a entrega do bem adquirido.

A título de exemplo, o Tribunal de Justiça do Paraná, em sede de apelação criminal, manteve a decisão condenatória referente a prática de estelionato em *site* de venda e compra:

> [...] o documento acostado às fls. 16 e os depoimentos das testemunhas perante a autoridade judicial demonstram com clareza solar que o acusado, visando a auferir vantagem ilícita, mediante meio fraudulento, induziu as vítimas em erro, consistente em anunciar no site de compras da internet "Mercado Livre", produtos com código de venda falso, pois os valores foram depositados, mas os objetos ofertados não foram entregues.[...] (TRIBUNAL DE JUSTIÇA DO PARANÁ. Apelação Criminal 748.706-5 / PR . Relator LUIZ ZARPELON. 4ª Câmara Criminal, data do julgamento 26/05/11, data da publicação/fonte dj 15/06/11).

Assim como no caso do crime de furto, por conta do sistema informático ser uma forma inovadora de se praticar o delito, o tipo penal de estelionato deve ser aplicado às condutas realizadas no mundo virtual, no que for compatível.

5.4 Invasão de Dispositivo Informático

Por conta de um caso ocorrido com uma pessoa pública em maio de 2012, em que fotos íntimas foram obtidas de modo ilegal e divulgadas sem autorização na Internet, novamente foram expostas as lacunas no ordenamento jurídico, em relação ao sistema informático e as condutas ilícitas praticadas por meio dele.

Com tamanha repercussão, o Legislativo, para dar uma resposta à sociedade, aprovou a Lei nº. 12.737/12 criminalizando condutas específicas em relação ao sistema informático, pois com a legislação até então vigente se fazia necessário algum resultado posterior, para que a punição do infrator fosse possível.

Visando antecipar a punição desses criminosos, foi criado o artigo 154-A do Código Penal, com o título de “Invasão de dispositivo informático” e com a seguinte redação:

> 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 [...]

Para sua consumação basta a realização de uma das condutas com uma das finalidades descritas no tipo penal, pois é um crime formal, podendo, ainda, configurar um crime mais grave caso haja a obtenção do resultado pretendido.

Além disso, o legislador, pretendendo dar maior eficácia ao novo tipo penal, complementou o *caput* do artigo 154-A com cinco parágrafos, que trazem figura equiparada, causa de aumento de pena das condutas do *caput*, figura qualificada e aumento de pena, bem como causas gerais de aumento de pena, conforme a redação do referido artigo:

> [...] § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Quanto à ação penal, o legislador julgou mais adequado ser pública, entretanto, no caso em que a vítima for um particular necessitará de representação para que tenha início a persecução penal.

Porém, na prática, o artigo 154-A parece um tipo penal de pouca aplicabilidade, pois se trata de um delito subsidiário, logo, a ocorrência de um crime mais grave, que é o que costuma ocorrer, implicará em sua absorção.

A título de exemplo, no caso em que da invasão resultar a obtenção de dados bancário, o infrator ao realizar saques incorrerá em furto qualificado; ou então se fosse obtido segredos do usuário e o infrator exigisse alguma vantagem para que não os divulgasse, ocorreria o crime de extorsão.

5.5 Interrupção ou Perturbação de Serviço Telegráfico, Telefônico, Informático, Telemático ou de Informação de Utilidade Pública

Por meio da Internet o deslocamento de dados e informações acontece de forma instantânea e uma prática muito comum no mundo virtual tem sido a paralização de *sites* de utilidade pública, sem qualquer motivo.

No entanto, o tipo penal existente que seria compatível com tal conduta era taxativo e, como sabido, não se admite analogia *in mallam partem*.

Visando atualizar o dispositivo, o legislador inseriu, em 2012, o parágrafo primeiro no artigo 266 do Código Penal.

Conforme explicação de Victor Eduardo (2013, p.649 e 650):

> O texto legal incrimina aqueles que provocam a interrupção total do serviço e também os que apenas prejudicam seu funcionamento. Pune, ainda, aqueles que, de algum modo, impedem ou criam óbices ao restabelecimento do serviço cujo defeito não foi por eles provocado.
> [...]
> O § 1º do art. 266 do Código Penal foi inserido pela Lei nº 12.737/13 e tem por finalidade punir os chamados "*crackers*" que, intencionalmente e em geral sem qualquer motivo (apenas por diversão), paralisam o funcionamento de *sites* de utilidade pública – Ministérios, Tribunais, empresas telefônicas ou de energia, da Receita Federal, de autarquias etc.

Por tutelar o interesse da coletividade se faz necessário a afetação do serviço em uma área considerável e ainda atingindo um número indeterminado de pessoa. Sua consumação ocorre com a prática de uma das condutas descritas no tipo penal.

Conforme observa Tarcisio Teixeira (2013, p.299):

> [...] o legislador [...] não empregou na redação do § 1º o termo "informático", como prevê o nome do crime. No entanto, a partir desta previsão legal, aquele que interromper serviço telemático de utilidade pública atenta expressamente contra a norma penal, sendo que a internet deve ser considerada como um serviço telemático de utilidade pública, haja vista a extrema relevância prestada às pessoas físicas e jurídicas, de direito público e privado. E mais, "telemático" significa a conjunção da telecomunicação com a informática, sendo esse o caso da Internet.

Como este crime pertence ao título "dos crimes contra a incolumidade pública" do Código Penal vigente e o tipo penal enfatiza que tem que ser serviço telemático ou de informação de utilidade pública, os serviços essencialmente privados não seriam protegidos por ele.

5.6 Pornografia Infantil

No momento que a Internet chegou ao alcance da população, transformou-se em um veículo de disseminação de pornografia.

No início apenas eram trocadas fotos, depois passou a existir interesse econômico com sites especializados em conteúdos pornográficos que ganhavam dinheiro com a venda de fotos e vídeos.

Todavia, alguns foram além e, aproveitando-se do anonimato que a Rede proporcionava aos usuários, utilizaram a Internet para divulgar materiais obscenos envolvendo menores de idade.

Conforme explicado pela ONG Safer Net Brasil (p.01):

> A Pedofilia é um distúrbio do comportamento classificado como uma Parafilia. As Parafilias representam diferentes formas de perversão sexual.
> [...]
> A Pedofilia é a atração sexual compulsiva por crianças e adolescentes. É classificada no DSM IV, livro que define os critérios de diagnóstico, no item F65.4 - 302.2.
> Pedofilia em si não pode ser tida como crime, ela é um transtorno da personalidade.
> Abuso de crianças e adolescentes praticado por pedófilos é considerado a prática criminosa.
> Portanto, a prática criminosa é a passagem ao ato: dos desejos impulsivos ao abuso sexual.
> O crime é o abuso de crianças ou produção de pornografia infantil.

Com o avanço tecnológico do sistema informático, o armazenamento e a divulgação de imagens e vídeos envolvendo pornografia infantil passaram a ser mais fáceis. Por conta disso, nos últimos anos o combate tem sido intensificado.

Em resposta aos infratores, os legisladores alteraram o Estatuto da Criança e do Adolescente, por meio da Lei nº. 11.829/08, que deu nova redação aos artigos 240 e 241, e também incluiu cinco novos artigos, do 241-A ao 241-E, visando ampliar o alcance do tipo penal.

O artigo 241-A faz questão de mencionar o sistema informático como sendo um dos meios para prática do delito, bem como o artigo 241-B passa a criminalizar a posse de material com pornografia infantil:

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente.
> Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente.

No entanto, mesmo com a atualização normativa e a integração de vários órgãos, públicos e privados, ainda é alta a divulgação de pornografia infantil, isso baseado na quantidade de denúncias realizadas diariamente, através da Internet.

Segundo informa a ONG Safer Net Brasil (Folha Uol, 2012, p.01):

> Casos de pornografia infantil dominam as denúncias de crime na Internet feitas no Brasil, de janeiro de 2006 a outubro de 2012, 40,5% do que foi denunciado no país supostamente abrigava conteúdo desse tipo.

Isso mostra o quanto ainda precisa o ordenamento jurídico evoluir e como se faz necessário a capacitação dos servidores, para melhor encararem essa nova realidade, pois o anonimato e outras facilidades encontradas no mundo virtual ainda trazem a sensação de impunidade, o que provavelmente deve encorajar os infratores a continuarem com suas atividades delituosas normalmente.

.

6 PERSECUÇÃO CRIMINAL

Com o avanço tecnológico a sociedade tem passado por grandes mudanças, pois houve reflexo em diversas áreas, como na comunicação, comércio, conhecimento e, como esperado, no Direito também.

As facilidades trazidas foram tanto boas quanto más. Para o bem surgiram vários equipamentos eletrônicos que otimizaram a prestação do serviço público, bem como os *sites* dos entes públicos, em que, por exemplo, funcionam as delegacias eletrônicas, o processo eletrônico nos fóruns, facilitando o acesso a justiça bem como o acompanhamento, tanto de investigação quanto de processo, para as partes interessadas.

No entanto, há o outro lado, a prática de diversos delitos, utilizando o sistema informático como um novo meio, assim como o surgimento de delitos específicos dessa nova tecnologia.

Isso causou uma impressão de que o ordenamento jurídico não estava preparado para combater esses infratores sem rosto, o que gerou forte sensação de impunidade, surgindo a ideia de que o mundo virtual era um lugar sem lei.

Entretanto, muitas das normas já existentes em nosso ordenamento jurídico são compatíveis, bastando adaptá-las a nova realidade, sem que violem os princípios constitucionais e penais, pois em muitos casos o sistema informático é empregado apenas como novo meio de praticar o crime.

Restando ao legislador atualizar o ordenamento jurídico, tanto para evitar a impunidade em relação às condutas existentes apenas no mundo virtual, quanto para melhorar a atuação das autoridades.

6.1 Polícia Judiciária

Com o avanço tecnológico foi criada a delegacia eletrônica. No Estado de São Paulo está localizada no sítio eletrônico da Secretaria de Segurança Pública, possibilitando a realização de boletim de ocorrência eletrônico de determinados delitos e de encaminhamento de *notitia criminis online* para a delegacia competente.

Outra inovação foi a criação da delegacia especializada em cibercrimes, para melhor atendimento das ocorrências que envolvam o universo virtual.

O problema é o fato de existirem poucas delegacias especializadas no país. A título de exemplo, a única existente no Estado de São Paulo encontra-se na capital, porém com área de atuação restrita a sua localidade.

Conforme declaração do delegado de polícia José Mariano de Araujo Filho (2012, p. 1):

> Investigadores policiais estão cada vez mais sem nenhum conhecimento técnico que os habilite a trabalhar nesta área, sendo rotineira a utilização de policiais que atuam em outras frentes de investigação para trabalharem com criminalidade eletrônica, principalmente em unidades situadas longe dos grandes centros onde ninguém sabe como recuperar e processar provas digitais.
> E para agravar ainda mais as questões relacionadas à falta de policiais com conhecimento técnico adequado e experiência na área, ainda existem outras relacionadas à cadeia de custódia das provas apreendidas, o que em última instância pode impedir que os dados recuperados venham a ser admitidos como prova.

Tal declaração enfatiza a importância da capacitação da Polícia Judiciária, pois a atuação em casos relacionados ao sistema informático exige o conhecimento técnico.

Não menos importante foi a questão levantada sobre o cuidado que se deve ter com as provas apreendidas. Em recente decisão o Superior Tribunal de Justiça evidenciou a importância da prova e a consequência de um descuido:

> [...] A regra básica da perícia criminal é a de que seu objeto seja preservado.
> Espécie em que os peritos flagrando no computador apreendido um 'vírus' conhecido como 'cavalo de tróia', excluíram-no do material a ser periciado, gerando incerteza acerca de sua potencialidade para invadir o equipamento e transmitir mensagens à revelia do usuário. [...] (SUPERIOR TRIBUNAL DE JUSTIÇA. Ação Penal 2011/0259587-8. Relator Ministro ARI PARGENDLER. Corte Especial, data do julgamento 03/04/13, data da publicação/fonte dje 09/04/13).

Isso nos mostra o quão delicadas são as situações relacionadas aos crimes de informática e como é preciso a colaboração do Poder Público com a Polícia Judiciária, seja por meio de atualização legislativa como por meio de estruturação da classe, pois erros cometidos durante a investigação podem gerar futuramente uma absolvição por falta de provas .

Mas, aos poucos o ordenamento jurídico tem sido atualizado, como, por exemplo, o art. 17-B da Lei nº. 12.683/12, que trata de desburocratização do acesso a dados cadastrais do investigado para melhorar o combate ao crime de lavagem de dinheiro:

> Art. 17-B. A autoridade policial e o Ministério Público terão acesso, exclusivamente, aos dados cadastrais do investigado que informam qualificação pessoal, filiação e endereço, independentemente de autorização judicial, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito.

Este novo artigo é uma grande mudança, pois assim as empresas terão que colaborar com as investigações, o que tornará o procedimento mais ágil, e sem que sejam violados os direitos do investigado, pois se tratam de dados objetivos, conforme descrito no referido dispositivo de lei.

No entanto, ainda se faz necessário a estruturação da Polícia Judiciária para o combate aos crimes de informática, tratada pelo art. 4º da Lei nº 12.735/12, seja realmente efetivada e que outras alterações legislativas sejam feitas, para adequar normas e criar novos tipos possibilitando maior eficácia à atuação dos órgãos públicos.

6.2 Poder Judiciário, Jurisdição e Competência

Assim como a Polícia Judiciária, os magistrados e seus servidores têm enfrentado problemas na aplicação da lei quando se trata de crimes de informática, por conta de suas peculiaridades.

Conforme explica o delegado de polícia José Mariano de Araujo Filho (2012, p. 1):

> [...] mesmo os magistrados necessitam ter um rol mínimo de conhecimento sobre a matéria, a fim de que consigam avaliar o mérito de um caso de cibercrime, pois se não tiverem conhecimento técnico suficiente para determinar que os elementos comprovadores de um delito estejam presentes, eles acabarão tendo que contar somente com opiniões divergentes apresentadas pelos advogados, promotores e seus peritos, sem realmente compreender a base do que for alegado. [...]

Ao consultar os sítios eletrônicos de tribunais, como o Tribunal Regional Federal da 3ª Região e o Superior Tribunal de Justiça, em busca de decisões a respeito de crimes de informática, percebe-se que muitas são referentes a conflitos de competência.

Mas para entender melhor porque isso tem ocorrido é preciso saber o que é jurisdição e o que é competência e ainda quais os critérios utilizados para resolver os conflitos internos e externos do país.

Nas palavras de Flávio Cardoso (2011, p. 91):

> Jurisdição é o poder-dever do Estado de aplicar a norma em abstrato ao caso concreto. Só o Estado, na função de Estado-juiz, é detentor do poder jurisdicional, por consequência, além de um poder, é também um dever, já que o monopólio obriga-o a agir quando um conflito lhe é apresentado. Em outras palavras, podemos dizer que a jurisdição é o poder de julgar um caso concreto, de acordo com o ordenamento jurídico, por meio do processo. Lembre-se de que a palavra 'jurisdição' vem do latim *juris* (direito) e *dictio* (dizer), significando então o 'poder de dizer o direito'.

No Brasil, para determinar se tem jurisdição, foi adotado o princípio da territorialidade temperada, em que, por questão de soberania, aplica-se a lei nacional aos crimes ocorridos dentro do território brasileiro e, excepcionalmente, aplica-se a lei estrangeira, quando ocorridas as condições previstas em lei.

Já para definição do lugar do crime é aplicada a teoria da ubiquidade, tornando maior o alcance da lei nacional.

No entanto, o espaço virtual abandona a tradicional concepção de território, uma vez que "caracteriza-se especialmente pelo fluxo de informação por meio de redes de comunicação." (CRESPO, 2011, p.117).

Por conta disso, torna-se difícil estabelecer a jurisdição, pois o ciberespaço não é propriamente um espaço, colocando em dúvida a eficiência das normas em vigor.

Outro problema, e que pode gerar a impunidade, é o fato de que os tipos penais existentes em um Estado nem sempre encontram correspondentes em outro Estado, o que pode dificultar a cooperação internacional, haja vista o caráter transnacional dos crimes virtuais, e até mesmo impossibilitar a extradição de um infrator.

Em se tratando de competência, que nada mais é do que a delimitação da jurisdição, os delitos no mundo virtual têm dado causa a diversos conflitos de competência entre a Justiça Federal e a Justiça Estadual.

Atento a isso, o deputado Ivo José apresentou o Projeto de Emenda à Constituição nº 407/05, o qual atribuía "à Justiça Federal o processamento de crimes praticados no âmbito da Internet ou em ambientes similares, disseminados em escala mundial". (Câmara dos Deputados, s. d., p. 1).

No entanto, o referido projeto de emenda foi arquivado em fevereiro de 2007, com fundamento no artigo 105 do Regimento Interno da Câmara dos Deputados[2].

Sem alteração legislativa e com constante aumento de ações relacionadas a delitos por meio do sistema informático, os tribunais têm sido forçados a se manifestarem sobre esse dilema.

Em recente decisão o Superior Tribunal de Justiça afirmou que:

> [...] 2. Para se firmar a competência da Justiça Federal, além da transnacionalidade do delito, deve-se demonstrar lesão a bens, serviços e interesses da União e que o País é signatário de acordos e tratados internacionais, a teor dos incisos IV e V do art. 109 da CF. [...] (SUPERIOR TRIBUNAL DE JUSTIÇA. CC 126768 / MG (CONFLITO DE COMPETENCIA 2013/0039050-5). Relatora Ministra Alderita Ramos de Oliveira (Desembargadora convocada do TJ/PE) (8215) órgão julgador s3 - terceira seção, data do julgamento 24/04/13, data da publicação/fonte DJe 10/05/2013).

Com isso, o Superior Tribunal de Justiça tem resolvido esses conflitos de competência, deixando claro que a Justiça Estadual, ainda que de forma residual, é competente para julgar delitos envolvendo o sistema informático.

Entretanto, a dificuldade de estabelecer o lugar da infração tem gerado conflitos internos também, seja entre comarcas e/ou subseções vizinhas ou até entre comarcas e/ou subseções de Estados diferentes.

---

[2] Art. 105. Finda a legislatura, arquivar-se-ão todas as proposições que no seu decurso tenham sido submetidas à deliberação da Câmara e ainda se encontrem em tramitação, bem como as que abram crédito suplementar, com pareceres ou sem eles, salvo as:
I - com pareceres favoráveis de todas as Comissões;
II - já aprovadas em turno único, em primeiro ou segundo turno;
III - que tenham tramitado pelo Senado, ou dele originárias;
IV - de iniciativa popular;
V - de iniciativa de outro Poder ou do Procurador-Geral da República.
Parágrafo único. A proposição poderá ser desarquivada mediante requerimento do Autor, ou Autores, dentro dos primeiros cento e oitenta dias da primeira sessão legislativa ordinária da legislatura subsequente, retomando a tramitação desde o estágio em que se encontrava.

Como não houve alteração até o momento nas normas processuais, o Poder Judiciário tem aplicado as regras existentes no Código de Processo Penal para solução dos conflitos.

Em um julgado referente ao crime de furto, o Superior Tribunal de Justiça decidiu da seguinte forma:

> O delito de furto mediante fraude, previsto no art. 155, § 4º, inciso II, do CP, consistente na subtração de valores de conta-corrente mediante fraude utilizada para ludibriar o sistema informatizado de proteção de valores mantidos sob guarda bancária, deve ser processado perante o Juízo do local da conta fraudada. [...] No caso, nota-se que inexiste qualquer ligação de conexão entre os fatos praticados no Rio de Janeiro e os demais fatos delituosos inseridos no banco de dados da Polícia Federal no Distrito Federal, investigados perante a Seção Judiciária do Distrito Federal, enfatizando a competência do Juízo da conta fraudada. A mera reunião de informações de inquéritos policiais diversos não atrai a competência do Juízo da localidade em que foi criado o Projeto Tentáculos, da Polícia Federal. 3. Conflito conhecido para declarar competente o suscitado, Juízo Federal da 8ª Vara Criminal da Seção Judiciária do Estado do Rio de Janeiro. (Superior Tribunal de Justiça. CC 119914 / DF (CONFLITO DE COMPETENCIA 2011/0274062-2). Relatora Ministra Alderita Ramos de Oliveira (Desembargadora convocada do TJ/PE) (8215) órgão julgador s3 - terceira seção, data do julgamento 12/12/2012, data da publicação/fonte dje 01/02/2013).

No caso em tela foi aplicado o artigo 70 do Código de Processo Penal para solucionar o conflito de competência entre os juízos federais do Rio de Janeiro e do Distrito Federal.

Contudo, durante o julgamento de um conflito de competência relativo ao crime de calúnia, houve divergência quanto à possibilidade de se estabelecer o local do crime. Por maioria dos votos o Superior Tribunal de Justiça entendeu que:

> [...] O crime de calúnia (art. 138, caput, do Código Penal) consuma-se no momento em que os fatos "veiculados chegam ao conhecimento de terceiros" (CC n. 107.088/DF, Relatora Ministra Maria Thereza de Assis Moura, DJe de 4/6/2010). 3. Tratando-se de queixa-crime que imputa a prática do crime de calúnia em razão da divulgação de carta em blog, na internet, o foro para processamento e julgamento da ação é o do lugar de onde partiu a publicação do texto tido por calunioso. 4. In casu, como o blog em questão está hospedado em servidor de internet sediado na cidade de São Paulo, é do Juízo da 13ª Vara Criminal dessa comarca a competência para atuar no feito. [...] (SUPERIOR TRIBUNAL DE JUSTIÇA. CC 97201 / RJ CONFLITO DE COMPETENCIA 2008/0150084-3 Relator Ministro CELSO LIMONGI (DESEMBARGADOR CONVOCADO DO TJ/SP) (8175). S3 - TERCEIRA SEÇÃO. Data do julgamento 13/04/11. Dje 10/02/12).

No entanto, como dito, a decisão não foi unânime, pois os Ministros Adilson Vieira e Napoleão Nunes entenderam que não era possível saber o lugar da infração.

Conforme explicam em seus votos:

> [...] (VOTO VOGAL) (MIN. ADILSON VIEIRA MACABU (DESEMBARGADOR CONVOCADO DO TJ/RJ)) Tem competência o juízo criminal do domicílio ou da residência do réu na hipótese em que o crime de calúnia foi cometido via internet e não se pode conhecer o lugar da infração, nos moldes da regra definida no artigo 72 do Código de Processo Penal. (VOTO VENCIDO) (MIN. NAPOLEÃO NUNES MAIA FILHO) Tem competência o juízo criminal escolhido pelo ofendido na hipótese em que o crime de calúnia foi cometido pela internet e não se sabe de onde foi emanado, pois o dano alcança todo o país, com repercussão em âmbito nacional, autorizando assim que o ofendido acione o ofensor em qualquer comarca do Brasil. (SUPERIOR TRIBUNAL DE JUSTIÇA. CC 97201 / RJ CONFLITO DE COMPETENCIA 2008/0150084-3 Relator Ministro CELSO LIMONGI (DESEMBARGADOR CONVOCADO DO TJ/SP) (8175). S3 - TERCEIRA SEÇÃO. Data do julgamento 13/04/11. Dje 10/02/12).

Como visto, o fato do servidor de Internet em que estava hospedado o blog localizar-se no Estado de São Paulo não foi argumento suficiente para o convencimento de todos os julgadores em relação ao estabelecimento do local do crime.

Em outro conflito de competência, dessa vez envolvendo pornografia infantil, os doutos julgadores reconheceram a impossibilidade de se estabelecer o local do crime, por conta do site em que o fato ocorreu ser internacional.

A solução do referido conflito foi a seguinte:

> [...] 1. No caso, não há divergências acerca da transnacionalidade necessária à determinação da competência da Justiça Federal, já que se trata de site de relacionamento internacional - OrKut – que possibilita a qualquer pessoa dele integrante o acesso dos dados constantes da página em qualquer local do mundo. 2. Não se olvida que a jurisprudência desta Corte posicionou-se no sentido de que o delito capitulado no art. 241, da Lei n. 8.069/1990 se consuma com o ato de publicação das imagens. Contudo, ao que se tem, na hipótese, configurada dúvida quanto ao local do cometimento da infração, pois não foi possível apurar de onde se partiu (local) a publicação das imagens e tampouco o responsável pela divulgação das fotos contendo pornografia infantil. 3. Ante a regra contida no § 2º do art. 72 do Código de Processo Penal, firmar-se-á a competência, no caso, pela prevenção, em favor do Juízo Federal de São Paulo onde as investigações tiveram início. 4. Conflito conhecido para declarar a competência do Juízo Federal da 8ª Vara Criminal da Seção Judiciária de São Paulo - SP, o suscitado. [...] (SUPERIOR TRIBUNAL DE JUSTIÇA. CC 130134 / TO (Conflito de Competência 2013/03173041). Relatora MINISTRA MARILZA MAYNARD (DESEMBARGADORA CONVOCADA DO TJ/SE). S3 – Terceira Seção. Data do julgamento 09/10/13. Dje 21/11/13).

Assim, de acordo como o crime praticado o grau de dificuldade em se estabelecer o local oscila.

Mas, mesmo com esses percalços, o Poder Judiciário não se isenta de fazer justiça, aplicando as regras dos artigos 69 e seguintes do Código de Processo Penal, de acordo com o caso em que se deparam.

7 CONCLUSÃO

No transcorrer do trabalho foi visto a evolução histórica do computador e da Internet e como tal desenvolvimento influenciou a vida das pessoas e o próprio Direito.

Além disso, foi abordado o risco que os usuários dessas tecnologias correm de terem sua intimidade e privacidade expostas, bem como os meios utilizados para que tal prática ocorra.

Também foram abordados os crimes de informática, trazendo conceito, classificação, sujeito ativo e passivo e estudado alguns dos delitos de alta ocorrência no mundo virtual.

E, para finalizar, foi analisado como tem sido realizada a persecução criminal.

Com base no presente estudo, foi possível concluir que tamanha foi a evolução que não havia como o legislador prever todas a situações geradas com o advento e popularização dessas tecnologias.

Todavia, embora fosse impossível de prever o impacto que causaria na vida das pessoas, o mundo virtual nunca foi sem regras.

Muito da legislação vigente é compatível, pois a tecnologia passou apenas a ser um novo meio de realizar situações já existentes, como comunicação, compras, crimes e etc.

Tanto a Polícia Judiciária quanto o Poder Judiciário tem mostrado que, mesmo com tantos obstáculos, como, por exemplo, o anonimato, a falta de estrutura

e profissionais sem conhecimento técnico, a lei tem alcançado e punido diversos infratores, reforçando que o mundo virtual tem leis assim como o mundo real.

Cabe ao legislador, com o tempo, atualizar o ordenamento jurídico, para que aquelas situações que surgiram após a criação do mundo virtual e que violam os direitos de outras pessoas não caiam na impunidade por conta da ausência de previsão legal.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDRADE, Wesley Almeida. **Crimes na Internet :** uma realidade na sociedade de informação. Presidente Prudente, 2006. Monografia (Graduação) - Faculdades Integradas "Antônio Eufrásio de Toledo", Faculdade de Direito de Presidente Prudente, 2006

BRASIL. Constituição (1988). **Comentários a Constituição Brasileira de 1988.** 2. ed., atual. e reform. São Paulo: Saraiva, 1997.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília: Senado, 1988.

BRASIL. Decreto-lei nº. 2.848, de 7 de dezembro de 1940. Código Penal. **Site do Planalto**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>. Acesso em: 22 jan. 2014.

BRASIL. Decreto-lei nº. 3.689, de 3 de outubro de 1941. Código de Processo Penal. **Site do Planalto**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm>. Acesso em: 22 jan. 2014.

BRASIL. Lei nº. 12.683, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. **Site do Planalto**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acesso em: 22 jan. 2014

BRASIL. Lei nº. 12.735, de 09 de julho de 2012. Altera a Lei nº 9.613, de 3 de março de 1998, para tornar mais eficiente a persecução penal dos crimes de lavagem de dinheiro. **Site do Planalto**. Disponível em:

< http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12683.htm>. Acesso em: 23 jan. 2014.

BRASIL. Lei nº. 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. **Site do Planalto**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 22 jan. 2014.

BRASILl. Resolução nº. 17, de 1989. Aprova o Regimento Interno da Câmara dos Deputados. **Site da Câmara dos deputados**. Disponível em: <http://www2.camara.leg.br/atividade-legislativa/legislacao/Constituicoes_Brasileiras/regimento-interno-da-camara-dos-deputados>. Acesso em: 21/01/14

.BRASIL. **Tribunal de Justiça do Paraná**. Apelação criminal. Condenação pelo crime de estelionato. Pleito que visa à absolvição. Não acolhimento. Elementos constitutivos do delito plenamente demonstrados. Agente que induziu a vítima em erro mediante venda pela internet de produtos que sabia de antemão não poder entregá- los. Conjunto probacional coeso e harmônico apontando para a configuração do delito. Sentença mantida. Recurso não provido. Apelação Criminal 748.706-5 / PR . Relator LUIZ ZARPELON. 4ª Câmara Criminal, data do julgamento 26/05/11, data da publicação/fonte dj 15/06/11. Disponível em: <http://portal.tjpr.jus.br/jurisprudencia/j/11119582/Ac%C3%B3rd%C3%A3o-748706-5>. Acesso em: 15 dez. 2013.

BRASIL. **Superior Tribunal de Justiça**. Conflito de competência. Delito de estelionato por meio da internet. Não incidência dos incisos IV e V da Constituição Federal. Competência da Justiça Estadual. Precedentes do STJ. CC 126768 / MG (CONFLITO DE COMPETENCIA 2013/0039050-5). Relatora Ministra Alderita Ramos de Oliveira (Desembargadora convocada do TJ/PE) (8215) órgão julgador s3 - terceira seção, data do julgamento 24/04/13, data da publicação/fonte DJe 10/05/2013. Disponível em: < http://www.stj.jus.br/SCON/jurisprudencia/toc.jsp?tipo_visualizacao=null&livre=conflito+de+compet%EAncia+internet&b=ACOR&thesaurus=JURIDICO>. Acesso em: 03 jan. 2014.

BRASIL. **Superior Tribunal de Justiça.** Conflito Negativo de Competência. Penal e Processo Penal. Fraude eletrônica na Internet. Transferência de numerário de conta da Caixa Econômica Federal. Furto mediante fraude que não se confunde com estelionato. Consumação. Subtração do bem. Aplicação do art. 70 do CPP. Competência da justiça federal paranaense. CC 67343 / GO (CONFLITO DE COMPETENCIA 2006/0166153-0). Relatora Ministra LAURITA VAZ (1120) órgão julgador s3 - terceira seção, data do julgamento 28/03/2007, data da publicação/fonte dj 11/12/2007, p.170. Disponível em: <http://www.stj.jus.br/SCON/jurisprudencia/toc.jsp?tipo_visualizacao=null&livre=67343&&b=ACOR&p=true&t=JURIDICO&l=10&i=11>. Acesso em: 03 dez. 2013

BRASIL. **Superior Tribunal de Justiça**. Conflito negativo de competência. Queixa-crime. Calúnia praticada, em tese, por jornalista. Carta publicada em blog. Lei de

imprensa. Norma não recepcionada pela constituição de 1988. Art. 70 do Código de Processo Penal. Competência do juízo suscitado. CC 97201 / RJ CONFLITO DE COMPETENCIA 2008/0150084-3 Relator Ministro CELSO LIMONGI (DESEMBARGADOR CONVOCADO DO TJ/SP) (8175). S3 - TERCEIRA SEÇÃO. Data do julgamento 13/04/11. Dje 10/02/12 Disponível em: <http://www.stj.jus.br/SCON/jurisprudencia/toc.jsp?tipo_visualizacao=null&livre=calunia+internet&b=ACOR&thesaurus=JURIDICO>. Acesso em: 21 jan. 14.

BRASIL. **Superior Tribunal de Justiça**. Penal. Crime de calúnia. Texto ofensivo veiculado pela 'Internet'. Ação Penal 2011/0259587-8. Relator Ministro ARI PARGENDLER. Corte Especial, data do julgamento 03/04/13, data da publicação / fonte dje 09/04/13. Disponível em: <http://www.stj.jus.br/SCON/jurisprudencia/toc.jsp?tipo_visualizacao=null&livre=calunia+internet&b=ACOR&thesaurus=JURIDICO>. Acesso: 19 jan. 14

BRASIL. **Superior Tribunal de Justiça**. PROCESSUAL PENAL. CONFLITO DE COMPETÊNCIA. PUBLICAÇÃO DE PORNOGRAFIA ENVOLVENDO CRIANÇA OU ADOLESCENTE ATRAVÉS DA REDE MUNDIAL DE COMPUTADORES - ORKUT. ART. 241 DO ECA. PECULIARIDADES DO CASO CONCRETO. DÚVIDAS QUANTO AO LOCAL DE ONDE EMANARAM AS IMAGENS PEDÓFILO-PORNOGRÁFICAS. ART. 72, § 2º, DO CPP. COMPETÊNCIA FIRMADA PELA PREVENÇÃO EM FAVOR DO JUÍZO ONDE AS INVESTIGAÇÕES TIVERAM INÍCIO. CC 130134 / TO (Conflito de Competência 2013/03173041). Relatora MINISTRA MARILZA MAYNARD (DESEMBARGADORA CONVOCADA DO TJ/SE). S3 – Terceira Seção. Data do julgamento 09/10/13. Dje 21/11/13. Disponível em: <http://www.stj.jus.br/SCON/jurisprudencia/toc.jsp?tipo_visualizacao=null&livre=pornografia+infantil++internet&b=ACOR&thesaurus=JURIDICO>. Acesso em: 21 jan. 14

BRAZ, Talita Solyon. **Direito à intimidade X Internet.** Presidente Prudente, 2007. 52 f. Monografia (Graduação) - Faculdades Integradas "Antônio Eufrásio de Toledo", Faculdade de Direito de Presidente Prudente, 2007

_____.**Normalização de apresentação de monografias e trabalhos de curso** – Presidente Prudente : Faculdades Integradas “Antonio Eufrásio de Toledo”, 2009.

CARDOSO, Marcel dos Santos. **Crimes virtuais e suas peculiaridades.** Presidente Prudente, 2008. Monografia (Graduação) - Faculdades Integradas "Antônio Eufrásio de Toledo", Faculdade de Direito de Presidente Prudente, 2008

CASTRO, Carla Rodrigues Araújo de. **Crimes de informática e seus aspectos processuais.** 2. ed., rev., ampl. e atual. Rio de Janeiro: Lumen Juris, 2003.

COELHO, Ana Carolina Assis. **Crimes virtuais:** análise da prova. 2008. Monografia (Graduação) - Faculdades Integradas 'Antônio Eufrásio de Toledo', Faculdade de Direito de Presidente Prudente, 2008.

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

DEGUCHI, Luís Gustavo Seki. **Violação dos direitos autorais na Internet.** Presidente Prudente, 2007. Monografia (Graduação) - Faculdades Integradas Antônio Eufrásio de Toledo, 2007

DINIZ, Maria Helena. **Código civil anotado.** 14. ed. São Paulo: Saraiva, 2009.

FILHO, José Mariano de Araujo. **Considerações sobre o caso Caso Carolina Dieckmann: a dura realidade de uma investigação.** Disponível em: <http://mariano.delegadodepolicia.com/consideracoes-sobre-o-caso-caso-carolina-dickeman-a-dura-realidade-de-uma-investigacao/>. Acesso em: 28 dez. 2013.

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

GLOSSÁRIO de Direitos Humanos. **Site SaferNet Brasil**. Disponível em: <http://www.ufsm.br/direito/artigos/ambiental/responsabilidade-dano-ambiental.htm>. Acesso em: 28 dez. 2013.

GONÇALVES, Victor Eduardo Rios; ESTEFAM, André. **Direito penal esquematizado:** parte geral. São Paulo: Saraiva, 2012.

GONÇALVES, Victor Eduardo Rios. **Direito penal esquematizado:** parte especial. Ed. Saraiva, 2013. 3ª edição.

GRECO, Rogério. **Código penal comentado.** 2. ed. Niterói: Impetus, 2009.

HISTÓRIA da Internet. **Site A.I.S.A., aprenda a Internet sozinho agora.** Disponível em: <http://www.aisa.com.br/historia.html>. Acesso em: 14 jan. 2014.

JESUS, Damásio Evangelhista de. **Direito penal:** parte geral. 30. ed. São Paulo: Saraiva, 2009.

_____. **Direito penal:** parte especial vol.2. 29. ed. São Paulo: Saraiva, 2009.

JUSTIÇA usa Código Penal para combater crime virtual. **Site do Superior Tribunal de Justiça.** Disponível em: <http://www.stj.gov.br/portal_stj/publicacao/engine.wsp?tmp.area=398&tmp.texto=90108>. Acesso em: 14 jan. 2014.

LEONARDI, Marcel. **Responsabilidade civil dos provedores de serviços de Internet.** 1. ed. São Paulo: Ed. Juarez de Oliveira, 2005.

LOUZADA, Roberta Guimarães. **O direito de privacidade em face aos meios eletrônicos.** Presidente Prudente, 2004. Monografia (Graduação) - Faculdades Integradas Antônio Eufrásio de Toledo, 2004

MACEDO, Viviane Poiato. **Da responsabilidade dos hackers e crackers no direito penal.** Presidente Prudente, 2004. Monografia (Graduação) - Faculdades Integradas "Antônio Eufrásio de Toledo", 2004.

MORAES, Alexandre de. **Direito constitucional.** 21. ed. São Paulo: Atlas S.a., 2007.

NOGUEIRA, Sandro D'Amato. **Crimes de informática.** 1. ed. Leme, SP: BH, 2008.

OLIVEIRA, Flávio Cardoso de. **Direito Processual Penal**. 5ª ed. Editora Saraiva. 2011. (Coleção OAB Nacional: primeira fase; 5)

PECK, Patricia. **Direito digital.** 5.ed. rev., atual. e ampl. São Paulo: Saraiva, 2013.

PEREIRA, Marcelo Cardoso. **Direito à intimidade na Internet.** Curutiba: Juruá, 2003.

PEREIRA, Marco Antonio Carvalho. **A Internet como ferramenta de trabalho do engenheiro químico**. Disponível em: <http://www.marco.eng.br/quimica/internet-eng-quimica.htm>. Acesso em: 14 jan. 2014.

PRADO, Luiz Regis. **Elementos de direito penal – volume 2 – parte especial.** São Paulo: Revista dos Tribunais, 2005.

PROJETOS de leis e outras proposições. **Site da Câmara dos Deputados**. Disponível: < http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=288142 >. Acesso: em 03 jan. 2014.

ROMANI, Bruno. Folha UOL. **Pornografia infantil domina denúncias de crime na internet no Brasil**. Disponível em: <http://www1.folha.uol.com.br/tec/1179545-pornografia-infantil-domina-denuncias-de-crime-na-internet-no-brasil.shtml>. Acesso em: 18 dez. 2013.

ROSA, Fabrízio. **Crimes de informática.** 1. ed. Campinas: Bookseller, 2002.

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

SANTOS, Claudomiro Júnior de Castro; Santos, Bruna Izídio de Castro e Gomes, Francisco José Dias. Direito à Privacidade no Âmbito da Internet – Aspectos Civis e Penais, de minha coautoria, apresentado no V encontro de Iniciação Científica, IV Encontro de Extensão Universitária e I Encontro de Iniciação Científica para o Ensino Médio, Vol. 5, Nº. 5 (2009), ISSN 21-76-8498, publicado na Revista Eletrônica Intertemas. Disponível em: <http://intertemas.unitoledo.br/revista/index.php/ETIC/article/viewFile/2084/2256> . Acesso em: 02 fev. 2014.

SANTOS, Fernando da Cruz Alves. **Aspectos relevantes da criminalidade através da informática.** Presidente Prudente, 2003. Monografia (Graduação) - Faculdades Integradas Antônio Eufrásio de Toledo, 2003.

TAKUSHI, Tiago Tadashi. **Crimes virtuais :** aspectos gerais, persecução criminal e de competência. Presidente Prudente, 2009. Monografia (Graduação) - Faculdades Integradas Antônio Eufrásio de Toledo, 2009

TEIXEIRA, Tarcisio. **Curso de direito e processo eletrônico:** doutrina, jurisprudência e prática. São Paulo: Saraiva, 2013.

TOMIZAWA, Guilherme. **A invasão de privacidade através da Internet.** Curitiba: JM, 2008.

VADE mecum RT. 4. ed., rev., ampl. e atual. São Paulo: Revista dos Tribunais, 2009.

VIANNA, Tulio Lima. **Fundamentos de direito penal informático:** do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Forense, 2003.