FACULDADE DE SABARÁ
AISLAN BRUNO DA SILVA MARTINS

CRIMES VIRTUAIS

SABARÁ
2017

AISLAN BRUNO DA SILVA MARTINS

CRIMES VIRTUAIS

Monografia apresentado como requisito parcial de avaliação do curso de Direito da Faculdade de Sabará para obtenção do título de Bacharel.

Professora Orientadora: Ma. Cláudia Leite Leonel

SABARÁ

2017

Sempre tive fé em Deus a quem tudo dedico nesta vida. Assim também a minha amada família, em especial aos meus pais pelo apoio, compreensão e incentivo que sempre depositaram em mim. A minha esposa pelo carinho, companheirismo e cumplicidade. Aos meus filhos Braian e a recém chegada a um mês Eulália, que seja este um grande incentivo para essa bela geração futura. Também, aos meus irmãos e sobrinhos queridos. Por fim, aos verdadeiros colegas de curso. Tudo termina com um novo começo.

RESUMO

Conforme a sociedade vai se evoluindo, o Direito se adapta às necessidades da mesma. Novas normas surgem conforme a conveniência, e assim com o avanço tecnológico estas normas também fazem com que o direito seja evoluído para que haja regularização do ambiente virtual no cotidiano das pessoas. Como em todo meio existe atos ilícitos, com o surgimento da internet e suas facilidades em propagação não seria distante o surgimento de crimes virtuais, sendo assim surgi a necessidade de adaptação do direito à nova realidade tecnológica da sociedade especialmente no âmbito penal e civil, não deixando de ter também ramificações para outras áreas do direito como o Eleitoral, Tributário, dentre outras. Sobre o tema crimes virtuais esta monografia expõe os delitos que começaram a ser praticados através da rede mundial de computadores tentamos aqui identificar como ocorrem tais crimes, quem são seus autores e o que o mundo jurídico relata sobre este tema, e a busca pelo amparo social através das legislação vigente dentro do que diz a legislação estrangeira e brasileira, verificando também o que existe hoje de projetos de lei sobre o assunto, devendo punir os indivíduos que usam da dificuldade de identificação da autoria para cometer diversos crimes.

Palavras-chave: Crimes virtuais. Crimes de Internet. Rede mundial de computadores. Cibercrime. Banco de dados. Crimes Informáticos

LISTA DE ABREVIATURAS E SIGLAS

ART – Artigo

CF/88 – Constituição da República Federativa do Brasil de 1988

CERT.BR – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.

CV – Crimes Virtuais

CC – Código Cívil

CP – Código Penal

IP – Internet Protocol

TCP – Transmission Control Protocol

WEB – Conjunto de páginas na internet

WWW – World Wide Web

SUMÁRIO

1 INTRODUÇÃO

A realização desta pesquisa tem como justificativa a possibilidade de utilização com fonte de conhecimento para a comunidade jurídica, principalmente na área do direito penal, buscando esclarecer e transpor conceitos sobre crimes virtuais.

A modernidade trouxe para dentro da sociedade a facilidade de comunicação e integração social mesmo que ainda de forma parcial contudo diversos locais no mundo podem hoje se comunicar através de equipamento eletrônicos pela rede mundial de computadores, a internet.

A rede mundial de computadores é utilizada com facilidade em vários campos da sociedade, como na educação, na política, no comércio, na ciência, bem como nas demais áreas.

Assim sendo o Direito como agente regulatório não ficaria ausente, pois, o processo de desenvolvimento global é inevitável e assim como os grupos citados, a evolução da sociedade é como um todo sempre acompanhada pelo Direito.

Atualmente o espaço virtual é amplamente utilizado para atividades comerciais e comunicação rápida entre pessoas em diversos pontos no mundo, o que torna este ambiente virtual lugar propício para prática de diversos tipos de delitos realizados através de informáticos pela rede mundial de computadores ou fora dela.

O presente trabalho visa expor o que está sendo feito para minimizar e neutralizar o avanço dos crimes virtuais, o que são estes crimes e como a sociedade moderna é uma vítima potencial quando está utilizando a internet para trafegar com pacotes de dados contendo informações pessoas e empresariais.

Outro objetivo da pesquisa é apresentar a classificação dos crimes virtuais conforme a doutrina versa sobre o tema e a classificação conforme a conduta do agente, buscando identificar quais os delitos virtuais mais praticados com o auxílio da rede

mundial de computadores e como o mundo jurídico através das leis estrangeiras e brasileiras tratam tais delitos.

Crimes virtuais ocorrem desde a década de 1970, embora o perfil do criminoso tenha mudado o número de usuários domésticos de informática aumentou desde então e com isso houve aumento de delitos.

Neste contexto, analisa-se que no mundo virtual em seus primórdios não havia fronteiras nem controle, sendo possível cometer crimes sem haver tipificação penal específica, que protegeria o usuário da rede mundial de computadores. A partir desde período surge também a intenção de coibir determinadas ações em função de atitudes delituosos praticadas através de equipamentos informáticos.

O Direito sempre está atrás do fato social, ou seja, o fato social acontece e logo em seguida o direito vem para regulamentar.

Cabe dizer que há dois pontos onde surgiu a necessidade de legislação específica no Brasil que regulamentasse a conduta dos usuários na rede mundial de computadores. No primeiro, o Marco Civil da internet, que regulamenta a relação civil das pessoas e o funcionamento dos serviços da internet, tendo por princípio a privacidade do usuário, das comunicações e a liberdade de expressão.
O segundo ponto, não menos importante, é a parte criminal, ou seja, determinar quais condutas praticada na internet são criminosas ou não.

Foi o que ocorreu com o Código Penal Brasileiro sofrendo alterações devido a lei 12.737/2012, mais conhecida como Lei Carolina Dieckmann.

A referida lei, criou uma tipificação nova, mas limitou muito a condenação por esse tipo penal, pois a lei 12.737/2012 só se aplica se este equipamento tiver habilitado nele um dispositivo de segurança. Portanto invadir computadores que não tenha senha ou dispositivos de segurança, ou software específico para este fim, ainda não é crime tipificado no Código Penal Brasileiro.

A metodologia aqui utilizada constitui em etapas concretas de investigação com finalidade mais restrita em termos de explicação geral dos fenômenos menos abstratos, será utilizado o Histórico, que consiste na investigação dos acontecimentos, processos e instituições do passado, verificando a sua influência na sociedade e suas mudanças tecnológicas. Através deste método, será feito um estudo sobre as formas de influência e como a evolução tecnológica interfere no comportamento social.

Perante leis adaptadas e fragilizadas tecnologicamente, seria a criação de leis mais severas uma questão mais eficaz contra os crimes virtuais?

Em um cenário geral o presente trabalho apresenta como estrutura em seus capítulos uma forma de entendimento de como surgiu o sistema Global de redes, os crimes informáticos e quais seus problemas, e as categorias destes crimes. Apresenta-se posteriormente capitulo sobre a competência para julgar tais crimes, a correspondente legislação nacional, lei Carolina Dieckmann e o Marco Civil da Internet. No próximo capítulo o entendimento da legislação internacional para crimes de informática e o as dificuldades do Brasil junto à Organização Mundial do Comércio no que diz respeito à lei 8.248/91, mais conhecida como lei de informática. E por fim versa sobre os obstáculos para obtenção de provas através de meios eletrônicos e a dificuldade para se rastrear aqueles que cometem tais delitos.

2 SISTEMA GLOBAL DE REDES

Desde o início da história da humanidade, o homem busca desenvolver novas ferramentas e tecnologias para facilitar o seu desenvolvimento e execução de tarefas laborais, buscando assim mais rapidez e superação. Assim sendo, o mundo passou por várias transformações, dentre elas destacamos a segunda grande guerra e a revolução industrial que notoriamente modificaram todo o mundo moderno e a forma de se viver e conviver neste planeta. Foi proporcionado assim maior interação do homem com a máquina. Não existe uma data específica que o sistema global de redes, ou na forma popular de dizer a internet moderna foi criada, mas essa surgiu em meados dos anos 1980.

A rede mundial de computadores, mais conhecida popularmente com internet ou simplesmente *web,* é um conjunto de várias outras redes que alicerçadas sobre um conjunto de protocolos (Internet Protocol Suite ou TCP/IP) e atendem a usuário de várias partes do mundo. Esses usuários podem ser milhões de pessoas físicas, órgãos governamentais, empresas privadas, fundações não governamentais, etc. que estão através de várias tecnologias de rede eletrônica interligadas.

Diversas sociedades diferentes iniciaram uma relação de proximidade, e a se comunicarem de forma mais eficiente, mas para isso ao se comunicarem via internet a cada usuário, sistema ou grupo de redes é atribuído um endereço único o que é chamado de IP. Diferenciando de uma tecnologia mais primaria como a telefonia.

ROHRMANN (2005, p. 4) relata que:

> A comunicação de dados através da internet não se dá pela mesma lógica da comunicação telefônica ordinária. Nesta última, uma vez estabelecida a ligação entre duas pessoas, o circuito se fecha, pois a comunicação ocorre como se houvesse uma ligação dedicada, exclusiva entre as duas pessoas. Esta tecnologia é conhecida como circuit switched (comutação por circuito).

Sob o IP, no entanto, vão circular várias informações e estas podem ser trocadas através de pacotes de dados o que torna a internet diferente da telefonia tradicional.

Essa troca de pacotes não é feita por um circuito fechado ou dedicado entre um receptor e um emissor. Toda mensagem ou arquivos trocados, vão passar por várias rotas e equipamentos de diversas tecnologias diferentes ao longo do sistema global de redes.

A década de 1990, marca o início da utilização da internet como ferramenta, não só de usuários ligados à área de pesquisa, mas estes usuários agora, pessoas naturais e jurídicas, começam a ter maior interesse pela internet devido a dois fatores essenciais.

O primeiro, foi a apresentação desta forma mais popular com a Teia de Alcance Mundial, mais conhecida como World Wide Web (www), após o surgimento de programas capazes de manipular interfaces gráficas tornando mais fácil e agradável a comunicação de dados pela internet. O segundo fator, e não menos fundamental, foi a necessidade de provedores de acesso aos serviços de internet, ou seja, empresas que possibilitassem que o público acessasse a internet.

Com a popularização do serviço e o aumento do tráfego de pacotes pela internet dia após dia, surge aí um dos principais problemas, há desta forma uma grande quantidade de informações muitas dela pessoais a disponíveis na rede, e estas ficam a disposição de milhares de usuários que possuem acesso ao serviço de internet. Estas informações caso não sejam disponibilizadas pelo próprio usuário, podem ser procuradas por um outro tipo de usuário que utilizam do mesmo serviço de internet para o cometimento de crimes, o chamados Crimes Virtuais ou Crimes Cibernéticos.

Em tempos atuais, a internet está relacionada às diversas áreas, com a velocidade na propaganda e a divulgação de serviços, empresas buscam melhorar suas vendas e aperfeiçoar seus produtos, pessoas físicas e jurídicas tem maior facilidade em oferecer e captar recurso físicos ou humanos.

O acesso a notícias, entre outros fatores que tornam a internet na sua forma mais popular é uma ferramenta de grande valor e abrangência em todo mundo, mas essa ferramenta composta de tantas vantagem também traz em sua forma usual vários

problemas que podem ser considerados desvantagens tais com a privacidade ou a falta dela o que deixa seus usuários expostos, a perda e desvio de informações sigilosas ou pessoais, ataques cibernéticos com a utilização ou não de vírus, ou seja, programas maliciosos desenvolvidos por programadores para que o equipamento do usuário não corresponda satisfatoriamente aos comandos do proprietário.

Vírus podem também fazer com que o equipamento forneça de forma indesejada acesso de terceiros ao computador de qualquer usuário, ou todo equipamento conectado a este em um ambiente de rede.

Outro grande desafio a ser superado pela internet é o aumento da criminalidade por acreditar alguns usuários em seu anonimato, seja em caráter de divulgação da pornografia, ameaças, pedofilia, dentre outros modos utilizados por criminosos virtuais.

Há relatos que os primeiros crimes virtuais ocorrem na década de 1970 onde especialistas em informática tinham o objetivo de enganar sistemas de segurança de instituições financeiras. Nos dias atuais o perfil dos criminosos logicamente não os mesmo dos daquela época, mas a principal mudança é que qualquer pessoa que tem acesso a internet tem capacidade de praticar um delito tendo como ferramenta principal a informática, sendo assim o usuário doméstico pode estar tanto no polo passivo ou no polo ativo em qualquer tipo de processo quem envolvam crimes cibernéticos.

2.1 CRIMES INFORMÁTICOS

Crimes informáticos é toda e qualquer atividade criminal que utilize uma infraestrutura baseada em tecnologia de informática. A prática deste tipo de crime é realizada através de qualquer equipamento informático tais com Tablets, SmartPhones, televisores, contudo a maioria destes delitos é efetuada através de computadores, seja através de acesso autorizado ou não a internet.

Pode-se conceituar o termo computador:

> Máquina capaz de receber, armazenar e enviar dados, e de efetuar, sobre estes, sequências previamente programadas de operações aritméticas (como cálculos) e lógicas (como comparações), com o objetivo de resolver problemas. (HOLANDA FERREIRA (2000, p.1016)

Crimes informáticos podem ser definidos como ações destrutivas a sistemas, interceptação de dados ou comunicações, modificação de dados, incitação ao ódio ou discriminação, terrorismo, transferência ilegal de dados, pedofilia, dentre outros.

São várias as denominações dadas a pratica de delitos em ambiente virtual, contudo não há consenso.

CRESPO descreve que:

> As denominações quanto aos crimes praticados em ambiente virtual são diversas, não há um consenso sobre a melhor denominação para os delitos que se relacionam com a tecnologia, crimes de computação, delitos de informática, abuso de computador, fraude informática, em fim, os conceitos ainda não abarcam todos os crimes ligados à tecnologia, e, portanto, deve-se ficar atento quando se conceitua determinado crime, tendo em vista que existem muitas situações complexas no ambiente virtual. (CRESPO, (2011, p.48)

Embora não haja acordo na doutrina quanto aos crimes praticados através de meios eletrônicos, vários doutrinadores os conceituam como “crimes digitais” A denominação deve ser realizada conforme o bem jurídico protegido, FRAGOSO assevera que: A Classificação dos crimes na parte especial do código é questão ativa, e é feita com base no bem jurídico tutelado pela lei penal, ou seja, a objetividade jurídica dos vários delitos ou das diversas classes de intenções. FRAGOSO (1983, p.5)

Portanto, ao verificar um delito como de informática é primordial uma verificação inicial, e ter a cautela se este é um crime digital ou não e daí sim aplicar o tipo penal correspondente, tendo em vista o bem jurídico tutelado.

3 DOS CRIMES DE INFORMÁTICA E SUAS CATEGORIAS

Atualmente, cresce o número de pessoas que acessam a internet.

Existem diversos *websites* na rede mundial de computares e a cada dia são criadas mais de mil homepages. Na internet atual é possível se encontrar basicamente de tudo desde comprar um livro até mesmo participar de uma graduação a distância, o que ocorre é que todo usuário que deste meio usufrui estão expostos aos mais variados crimes pois não há barreiras concretas para que estes deixem de perpetuar por toda rede causando imensos estragos no cotidiano dos internautas de boa fé.

Constatar e classificar um crime virtual não é tarefa simples e fácil, pois ainda são poucas as conclusões existentes. O fato se deve a tecnologia, que evolui rapidamente e a opinião dos legisladores segue no mesmo ritmo.

Alguns criminosos utilizam computadores para cometer de crimes, porém há casos que sem a informática não seria lógico o cometimento de determinados crimes.

Neste sentido Crespo (2011, p.60) referenciando a Tiedemann que formulou em 1980 as classes dos delitos de informática:

> a) Manipulações: podem afetar o input (entrada), o output (saída) ou mesmo o processamento de dados;
> b) Espionagem: subtração de informações arquivadas abarcando-se, ainda, o furto ou emprego indevido de software;
> c) Sabotagem: destruição total ou parcial de programas;
> d) Furto de tempo: utilização indevida de instalações de computadores por empregados desleais ou estranhos.

GRECO FILHO (2000, p.85) fraciona as classes da seguinte forma tendo em vista condutas contra sistemas de informática e condutas contra outros bens jurídicos:

> Focalizando-se a Internet, há dois pontos de vista a considerar: crimes ou ações que merecem incriminação praticados por meio da internet e crimes ou ações que merecem incriminação praticados contra a Internet, enquanto bem jurídico autônomo. Quanto ao primeiro, cabe observar que os tipos penais,

> no que concerne à sua estrutura, podem ser crimes de resultado de conduta livre, crimes de resultado de conduta vinculada, crimes de mera conduta ou formais (sem querer discutir se existe distinção entre estes) e crimes de conduta com fim específico, sem prejuízo da inclusão eventual de elementos normativos. Nos crimes de resultado de conduta livre, à lei importa apenas o evento modificador da natureza, com, por exemplo, o homicídio. O crime, no caso, é provocador o resultado morte, qualquer que tenha sido o meio ou a ação que o causou.

Já o Dr. VLADIMIR ARAS (2001, p.51), aborda a divisão de outra forma:

> a) uma primeira, onde estão substancialmente unidos pela circunstância que o computador constitui a necessária ferramenta de realização pela qual o agente alcança o resultado legal;
> b) a segunda categoria de crimes do computador, poderia incluir todos aqueles comportamentos ilegítimos que contestam os computadores, ou mais precisamente, seus programas;
> c) a última categoria deveria juntar todas as possíveis violações da reserva sobre a máquina. Aqui entram em consideração as habilidades de colheita e elaboração de todo tipo de dados.

Existem distinções em todas classificações expostas contudo há também pontos em comum, alguns posicionamentos têm como objeto protegido os meios eletrônicos, ou seja, o bem jurídico e outras como o meio eletrônico com forma ou instrumento de lesionar outros bens jurídicos tornando esta última um entendimento que abarca mais acerca das práticas.

Vários autores usam o termo “crime” quando falam de condutas lesivas a sistemas informáticos, a dados ou informações.

4 CRIMES POR MEIO ELETRÔNICO E INTERNET

Verificar condutas criminosas que se propagam pela internet é uma tarefa delicada, pois é difícil localizar onde o agente que efetuou o crime se encontra pois a prática destes delitos não encontram barreiras pela internet e circulam livres pelo sistema global de comunicação mundial.

A maioria destas ações delituosas ocorrem tanto pela rede quanto pelo mundo real, porém alguns crimes têm certas peculiaridades o que torna necessário uma adequação quanto ao seu tipo penal

4.1 INVASÃO E PRIVACIDADE

Com a maior participação de usuário na rede mundial de computadores, começou a ser propagado de forma bem ampla um número ilimitado de informações nesta rede, tanto informações que são inseridas através de cadastro em sites comerciais, quanto preenchimento de formulários eletrônicos para através de perfis para adesão a redes sociais.

Os usuários utilizam a internet para acesso a diversos tipos de informações, pois a rede mundial de computadores possibilita a realização de várias atividades, o que ocorre é que todas informações disponibilizadas com ou sem autorização pela internet, podem trazer penalidades a pessoas jurídicas ou físicas que usam destas informações sem consentimento.

O código civil brasileiro também garante a proteção da privacidade, assim como também a Constituição Federal (CF), quem em seu artigo 5º, X, garante a qualquer cidadão que não tenha a sua privacidade respeitada, o direito a reparação, sendo aquela considerada inviolável.

> 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:
> X - 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;

O que se deve é resguardar o cidadão também no que diz respeito aos seus dados disponibilizados na internet, sejam eles inseridos através de órgãos públicos, comercio eletrônico ou até mesmo através de entes privados. Informações pessoais de qualquer pessoa natural ou jurídica não deveriam ser tratadas como mercadorias desconsiderando assim seus aspectos objetivos. Ë dever do Estado garantir ao cidadão o direito de proteção a sua identidade, e que dados disponibilizados sejam usados somente para um objetivo específico.

4.2 ESPIONAGEM ELETRÔNICA

Atualmente, a utilização de tecnologias da informática por pessoas é crescente, com isso também cresce a dependência das empresas por softwares diversos, o que eleva o tempo de conexão de ambas situações a rede mundial de computadores, ocasionando o lançamento elevado de informações estratégicas e pessoais nos servidores empresariais. Essa prática aumenta a necessidade de prevenção e monitoramento da segurança da informação.

O Código Penal não tipifica de forma específica o crime de espionagem eletrônica, sendo que a conduta este definida no Código Penal em seus artigos 154 e 154A

> Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem: Pena – detenção, de três meses a um ano, ou multa.
>
> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com 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 três meses a um ano, ou multa.

A CLT versa em seu artigo 482, “g” que o funcionário que o funcionário que praticar a conduta poderá ter seu contrato rescindido:

> Constituem justa causa para rescisão do contrato de trabalho pelo empregador:
> g) violação de segredo da empresa.

Em ambiente laboral, deve-se haver mais segurança através de investimentos por parte das empresas, tendo em vista que ameaças internas são mais difíceis de serem rapidamente identificadas, pois o agente que exerce tal conduta é um usuário considerado legítimo evitando seu rastreamento.

Patrícia Peck (2010, p. 385) nos diz que:

> "É primordial a aplicação de medidas em três níveis, físico, lógico e comportamental para o combate a espionagem, alguns pontos devem ser observados tais como controles mais rígidos dos insider; Frequência e controle de acesso em conjunto com a máquina; Uso de softwares de monitoramento; regulamentação de equipamentos moveis e bloqueio de portas USB; Criação de canal de denúncia; Garantia de acesso somente a que é necessário; realização de testes de vulnerabilidade."

4.3 FRAUDES VIRTUAIS

Comprar, vender, jogar, se relacionar, trabalhar, a internet moderna proporciona aos seus usuários a interação em tempo real, ferramentas com e-mail e chat que são constantemente utilizados de forma pratica e rápida por todos usuário da rede. Da mesma forma, a navegação web e os games podem proporcionar lazer e acesso à educação de forma interativa.

Em crimes definidos como Fraude Virtual, a conduta aplicada é a de invasão, modificação ou alteração, adulteração em sistema de processamento de dados ou supressão de dados eletrônicos ou programas.

O CERT-BR (Centro de estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil) diz que fraude eletrônica se dá por: Mensagem não solicitada afim de se passar por instituição conhecida ou ainda a mensagens que induzem o usuário a instalar de códigos de origem duvidosa. (Disponível em https://www.cert.br/, acessado em 10 de nov. 2017)

Fraudes virtuais possuem duas modalidades: As fraudes externas, onde quem comete a fraude não tem vínculo direto com o local a ser fraudado e a fraude interna que é cometida por aquele infrator que está dentro do local a ser fraudado seja ele um morador ou empregado ou mesmo um terceiro que esteja prestando serviço ou de passagem pelo local.

Na prática dos crimes envolvendo fraudes virtuais, o usuário é induzido a fornecer seus dados financeiros ou pessoais. Parte das ações atualmente praticadas, os fraudadores tentam através das redes sociais maneiras de convencer usuários a fornecer dados pessoais.

4.4 CRIMES CONTRA A HONRA

Qualidades físicas, morais e intelectuais de um indivíduo são a sua honra. A honra deve ser protegida pois é um patrimônio que a pessoa possui.

A honra do indivíduo é subjetiva, constituída por sentimentos próprios de respeito, de moral, de atributos intelectuais e por alguns outros elementos.

Crimes contra a honra estão previstos no código penal brasileiro e estes são os crimes mais comuns cometidos através da internet.

O crime de difamação é um dos crimes contra a honra, este está definido no artigo 139 do código penal: Difamar alguém, imputando-lhe fato ofensivo à sua reputação: Pena – Detenção, de 3 (três) meses a 1 (um) ano, e multa.

Difamar é um tipo de crime que ataca a honra objetiva da pessoa, este crime é praticado na internet em diferentes formas tanto imputando ao indivíduo algum fato que ofenda sua honra objetiva através de e-mail ou até mesmo publicando ofensas em redes sociais.

No artigo 139 do código penal, a norma é destinada a pessoa humana, logo o crime de difamação a pessoa jurídica não pode ser sujeito passivo, neste caso pode se aplicar a lei nº 5.250/67 – Lei de Imprensa INELLAS (2004, p.51).

Diferente do crime de calúnia no art. 138 do Código Penal Brasileiro, o Crime de difamação não exige que a atribuição seja falsa bastando somente o agente sentir sua honra ofendida perante a sociedade e o crime se consuma no momento em que o terceiro toma conhecimento do fato, já em ambiente virtual o crime irá se consumar, por exemplo, quando houver a propagação do ato ofensivo através das redes sociais.

O Crime de Calúnia está descrito no art. 138 do Código Penal, o qual versa: Caluniar alguém, imputando-lhe falsamente fato definido como crime. Pena – Detenção de 6 (seis) meses a 2 (dois) anos, e multa.

No crime de Calúnia o agente imputa a alguém um crime e abala sua reputação frente a sociedade abalando assim sua honra objetiva.

Já o crime de injúria, que está previsto no artigo 140 do código penal, o agente propaga de forma negativa uma qualidade da vítima, qualidade esta que diga respeito aos seus atributos morais, físicos ou intelectuais ofendendo de forma subjetiva a hora da vítima.

4.5 PORNOGRAFIA INFANTIL

Pedofilia é um ato de perversão que leva um indivíduo já em fase de vida adulta a se sentir sexualmente atraído por crianças ou mesmo a prática de atos sexuais com estas.

A pedofilia há anos aflige o mundo, mas com a popularização da internet ficou mais em evidência, levando ser mais estudada e analisada no âmbito jurídico e psicológico. Apesar de ser causa de repúdio por boa parte da sociedade, infelizmente, há na internet diversas figuras com este tipo de material.

O código penal, em seu artigo 234, versa:

> Fazer, importar, exportar, adquirir ou ter sob sua guarda, para fim de comércio, de distribuição ou de exposição pública, escrito, desenho, pintura, estampa ou qualquer objeto obsceno:
> Pena – detenção, de 6 (seis) meses a 2 (dois) anos, ou multa.
> Parágrafo único. Incorre na mesma pena quem:
> I – vende, distribui ou expõe à venda ou ao público qualquer dos objetos referidos neste artigo;
> II – realiza, em lugar público ou acessível ao público, representação teatral, ou exibição cinematográfica de caráter obsceno, ou qualquer outro espetáculo, que tenha o mesmo caráter;
> III – realiza, em lugar público ou acessível ao público, ou pelo rádio, audição ou recitação de caráter obsceno.

O elemento subjetivo aqui é o dolo, pois o infrator tem o objetivo de comercializar o objeto material do crime ou mostrar ao público, a disponibilização do material ou possibilidade de alguém ter acesso ao mesmo já configura a pratica deste delito.

Na Pedofilia existe uma perversão sexual pois o adulto se relaciona de forma erótica com crianças ou adolescentes, já na Pornografia infantil não é necessário que haja relacionamento, bastando somente a divulgação ou comercialização de material erótico envolvendo crianças ou adolescentes.

A lei 8.069/90, O Estatuto da Criança e do Adolescente, tipifica esse tipo penal em seu artigo 241, II sendo considerado crime a divulgação/publicação de imagem contendo material pornográfico de crianças ou adolescente, estabelecendo penalidades ao pedófilo e todo aquele que comercializa material de pornografia infantil.

O ECA assim versa:

> Art. 240 – Produzir ou dirigir representação teatral, televisiva ou película cinematográfica, utilizando-se de criança ou adolescente em cena de sexo explícito ou pornográfica:
> Pena – reclusão de 1 (um) a 4 (quatro) anos, e multa.
> Parágrafo único. Incorre na mesma pena que, nas condições referidas neste artigo, contracena com criança ou adolescente.
> Art. 241 – Fotografar ou publicar cena e sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão de 1 (um) a 4 (quatro) anos.

O Supremo Tribunal Federal entende que basta a divulgação e o crime já está consumado independente do meio utilizado. Entendimento da Colenda da Primeira turma do STF:

> ESTATUTO DA CRIANÇA E DO ADOLESCENTE – Art. 241 – Inserção de cenas de sexo explícito em rede de computadores (Internet) – Crime caracterizado – Prova pericial necessária para apuração da autoria. “Crime de computador”; publicação de cena de sexo infanto-juvenil (E.C.A., art. 241), mediante inserção em rede BBS/Internet de computadores atribuída a menores – Tipicidade – Prova pericial necessária à demonstração da autoria – Habeas Corpus deferido em parte.
>
> 1. O tipo cogitado – na modalidade de “publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente” – ao contrário do que sucede por exemplo aos da Lei de Imprensa, no tocante ao processo da publicação incriminada é uma normal aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador.
> 2. Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta incriminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da Lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo.
> 3. Se a solução da controvérsia de fato sobre a autoria da inserção incriminada do conhecimento do homem comum, impõe se a realização de prova pericial.

Muitas vezes, uma perícia técnica rigorosa deve analisar as provas eletrônicas para que essas sejam aceitas em processo.

Contudo conclui-se que a exposição de uma criança ou adolescente de forma pornográfica na internet tem como pena a reclusão de 2 a 6 anos e multa.

4.6 ESTELIONATO

O estelionato é uma das práticas de crime mais popular do nosso ordenamento jurídico, o número de pessoas que tentam adquirir para si ou para outro vantagens ilícitas, aumenta tanto com o uso da internet quanto fora dela. As condutas variam conforme os meios eletrônicos disponíveis.

O código penal em seu artigo 171 assevera que:

> Art. 171. Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa.

Pela internet é comum um estelionatário utilizar condutas típicas tal com encaminhar para um usuário qualquer um e-mail com conteúdo falso fazendo o destinatário acreditar que ao acessar o link enviado no corpo deste e-mail o mesmo será direcionado para um site confiável afim de atualizar seus dados cadastrais, tendo assim o criminoso formas de adquirir informações pessoais ou confidenciais daquele usuário. Na maioria das vezes essa prática ocorre para apropriação de dados bancários.

Existem formas na rede mundial de computadores de tentar se livrar destes e-mails indesejados, uma destas formas seria a atualização de sistemas de proteção como *Firewall* e Antivírus, o qual servirão de barreiras para potenciais intrusos controlando, assim, as regras de transferência de documentos.

4.7 DANO INFORMÁTICO

O código penal Brasileiro prevê o crime de dano, em seu artigo 163, que versa:Art.163: Destruir, inutilizar ou deteriorar coisa alheia:Pena – detenção, de um a seis meses, ou multa.

No código penal brasileiro, o legislador protege o dano a “coisa” seja ela móvel ou imóvel contudo “coisa” denota algo que pode ser tocada, ou seja real. A época da elaboração do artigo 163 do CP o legislador não considerou o dano informático e nos dias atuais ao aplicar a conduta do agente a conduta é relacionada a algo tangível como por exemplo computadores, servidores, *pen drivers, hard disks*, contudo não há a deterioração destes mas sim nos dados e informações eletrônicas nele contidos.

Não se pode aqui falar em uma interpretação analógica, tendo em vista que a mesma seria *in malam partem*, o que não poderia ser feito, tendo em vista o princípio da legalidade, que proíbe a utilização de analogia no Direito Penal em situações que tragam prejuízos ao agente da conduta.

É impossível algo que é imaterial como material e hoje quando alguém pratica um dano informático a um terceiro mesmo que de forma dolosa este agente não tem conduta específica tipificada, não estando sujeito as penas do código penal, sendo responsabilizado somente pelo que dispõe o código civil brasileiro.

4.8 CRIMES CONTRA A PROPRIEDADE INTELECTUAL

Não há fiscalização efetiva na internet, também não existe territorialidade, sendo assim a circulação de informações é rápida permitindo que materiais sejam copiados e distribuídos de forma desordenada ou causando desrespeito a quem o criou, não dando respaldo ao autor da obra.

O Art. 184 do Código Penal versa:

> Art. 184 - Violar direitos de autor e os que lhe são conexos: Pena - detenção, de 3 (três) meses a 1 (um) ano, ou multa.
> § 1º - Se a violação consistir em reprodução total ou parcial, com intuito de lucro direto ou indireto, por qualquer meio ou processo, de obra intelectual, interpretação, execução ou fonograma, sem autorização expressa do autor, do artista intérprete ou executante, do produtor, conforme o caso, ou de quem os represente: Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
> § 2º - Na mesma pena do § 1º incorre quem, com o intuito de lucro direto ou indireto, distribui, vende, expõe à venda, aluga, introduz no País, adquire, oculta, tem em depósito, original ou cópia de obra intelectual ou fonograma reproduzido com violação do direito de autor, do direito de artista intérprete ou executante ou do direito do produtor de fonograma, ou, ainda, aluga original ou cópia de obra intelectual ou fonograma, sem a expressa autorização dos titulares dos direitos ou de quem os represente.
> § 3º - Se a violação consistir no oferecimento ao público, mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção da obra ou produção para recebê-la em um tempo e lugar previamente determinados por quem formula a demanda, com intuito de lucro, direto ou indireto, sem autorização expressa, conforme o caso, do autor, do artista intérprete ou executante, do produtor de fonograma, ou de quem os represente: Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
> § 4º O disposto nos §§ 1º, 2º e 3º não se aplica quando se tratar de exceção ou limitação ao direito de autor ou os que lhe são conexos, em conformidade com o previsto na Lei nº 9.610, de 19 de fevereiro de 1998, nem a cópia de obra intelectual ou fonograma, em um só exemplar, para uso privado do copista, sem intuito de lucro direto ou indireto.
> Art. 186 - Procede-se mediante:
> I – queixa, nos crimes previstos no caput do art. 184;
> II – ação penal pública incondicionada, nos crimes previstos nos §§ 1º e 2º do art. 184; III – ação penal pública incondicionada, nos crimes cometidos em desfavor de entidades de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo Poder Público;
> IV – ação penal pública condicionada à representação, nos crimes previstos no § 3º do art. 184.

Violação de programas de computador não é mencionado no código penal brasileiro, que se limita a cópias de obras intelectuais e a obras fonográficas

A pirataria de softwares é, atualmente, a forma mais comum de violação de direito autoral e consiste na cópia não autorizada de softwares que são feitas por empresas ou usuários finais.

A rede mundial de computadores tem hoje diversos sites ao redor do mundo que disponibilizam download gratuito de software, oferecendo ao usuário que navega na rede copias desviadas ou falsas, favorecendo assim a pirataria pela internet.

Os operadores do direito têm um grande desafio, pois o modelo econômico de exploração de propriedade intelectual deve ser repensado, pois na atualidade a ideia que se tem é que se está publicado na internet é público.

5 COMPETÊNCIAS PARA PROCESSAR E JULGAR

De forma essencial, abordando o conceito de jurisdição que é o poder que o Estado concede ao Juiz de aplicar o direito no caso concreto aplicando a lei a cada caso. Já a competência, assim como o Estado concede ao Juiz o poder de dizer o direito, este também limita o poder, ou seja, a competência é o limite da Jurisdição do Juiz. A competência é a área de atuação do juiz

Crimes virtuais podem ser praticados em qualquer lugar do mundo que haja acesso à internet e o acesso pode ser realizado não somente através de computadores, mas também através de smartphones, televisores e demais equipamentos informáticos. Devido a mobilidade dos equipamentos torna-se complexo determinar qual juiz é competente para julgar, não há legislação que norteie para estes casos

Nos casos de crimes praticados no Brasil, o Código de Processo Penal Brasileiro diz que:

> Art. 70. A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução.
> § 1o Se, iniciada a execução no território nacional, a infração se consumar fora dele, a competência será determinada pelo lugar em que tiver sido praticado, no Brasil, o último ato de execução.
> § 2o Quando o último ato de execução for praticado fora do território nacional, será competente o juiz do lugar em que o crime, embora parcialmente, tenha produzido ou devia produzir seu resultado.
> § 3o Quando incerto o limite territorial entre duas ou mais jurisdições, ou quando incerta a jurisdição por ter sido a infração consumada ou tentada nas divisas de duas ou mais jurisdições, a competência firmar-se-á pela prevenção

Os crimes internacionais que se iniciaram no Brasil, mas progrediram para fora desde, são de competência da Justiça Federal.

A lei 7.209 de 11 de julho de 1984 no seu artigo 5º e 6º nos diz que:

> Art. 5º - Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional.

> § 1º - Para os efeitos penais, consideram-se como extensão do território nacional as embarcações e aeronaves brasileiras, de natureza pública ou a serviço do governo brasileiro, onde quer que se encontrem, bem como as aeronaves e as embarcações brasileiras, mercantes ou de propriedade privada, que se achem, respectivamente, no espaço aéreo correspondente ou em alto mar.
> § 2º - É também aplicável a lei brasileira aos crimes praticados a bordo de aeronaves ou embarcações estrangeiras de propriedade privada, achando-se aquelas em pouso no território nacional ou em voo no espaço aéreo correspondente, e estas em porto ou mar territorial do Brasil.
> 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.

Portanto, para os crimes praticados através da internet, é de suma importância observar sempre onde ocorreu o fato criminoso. Caso este local não possa ser detectado a competência ficará a cargo do Juízo que iniciou as investigações. Havendo hipótese de transnacionalidade do crime virtual, este será de competência da Justiça Federal.

6 LEGISLAÇÃO NACIONAL EM RELAÇÃO AOS CRIMES VIRTUAIS

Os primeiros atos legislativos no Brasil ocorreram através do Plano Nacional de Informática e automação realizado elaborado através da Lei 7.232 de 1984 que dispunha sobre diretrizes de informática em território Brasileiro. Logo depois foi elaborada a lei número 7.646 de 1987, sendo revogada pela lei 9.609 de 1998 sendo que esta foi a primeira a descrever em seu ordenamento infrações de informática.

Ainda há outras leis, mediadas provisórias, decretos, portarias e resoluções que versam sobre o tema, dentre várias podemos citar:

Projeto de lei 2.126 de 2011 transformado em Lei ordinária de 12.765 de 2014, estabelecendo princípios, garantias e deveres para o uso da internet no Brasil. Conhecido como Marco civil da Internet.

Lei 8.248 de 23 de outubro de 1991 que versa sobre a capacitação e competitividade do setor de automação e de informática.

Resolução CNJ número 41 de 11/09/2007, com publicação no DJ de 14/09/2007, que fala sobre a utilização do domínio “jus.br” pelo poder judiciário.

Instrução Normativa do Tribunal Superior do Trabalho número 30 de 13 de setembro de 2007 que regulamenta o âmbito da justiça do trabalho, a lei 11.419 que versa sobre a informatização do processo judicial.

Resolução do Supremo Tribunal de Justiça número 9 de 5 de maio de 2007, que altera o artigo 1º da resolução número 2 de 24 de abril de 2007, que versa sobre o recebimento de petição eletrônica no âmbito do STJ.

Lei 11.829 de 25 de novembro de 2008, publicada no Diário Oficial da União que altera a lei 8.069 de 13 de Julho de 1990, o ECA Estatuto da Criança e do Adolescente que

versa sobre pornografia infantil e demais condutas praticadas a pedofilia através da internet.
Lei 12.034 de 29 de setembro de 2009, publicada no Diário Oficial da União em 30 de setembro de 2009 que alterou a lei 9.096 de 1995, Lei dos Partidos Políticos, a lei 9.504 de 30 de setembro de 1997 estabelecendo normas para as eleições e a lei 4.737 de 15 de julho de 1965, o Código Eleitoral.

Lei 10.176 de 11 de janeiro de 2001 que altera a Lei nº 8.248, de 23 de outubro de 1991, a Lei nº 8.387, de 30 de dezembro de 1991, e o Decreto-Lei nº 288, de 28 de fevereiro de 1967, versando sobre a capacitação e competitividade do setor de tecnologia da informação.

Lei número 11.077 de 30 de dezembro de 2004 que modifica a Lei nº 8.248, de 23 de outubro de 1991, a Lei nº 8.387, de 30 de dezembro de 1991, e a Lei nº 10.176, de 11 de janeiro de 2001, dispondo sobre a capacitação e competitividade do setor de informática e automação dando outras providências.

Lei número 13.023/14 que modifica a Leis número 8.248/1991, a 8.387/1991, e revoga dispositivo da Lei número 10.176/2001, para dispor sobre a prorrogação de prazo dos benefícios fiscais para a capacitação do setor de tecnologia da informação.

Lei 10.408 de 10 de janeiro de 2002 que altera a lei 9.504 de 1997 estabelecendo normas para a ampliação de segurança e fiscalização do voto eletrônico.

A medida provisória número 534 que alterou o artigo 28 da lei número 11.196 de 2005 para inclusão digital Tablet PC produzido no Brasil para inclusão digital do governo federal.

Conforme evolui a sociedade e a busca por facilidades, o direito vai necessitar também de uma constante adaptação das normas, por isso há uma constante mudança em nosso ordenamento jurídico no que se refere a informática e os crimes através dela praticados.

6.1 LEI CAROLINA DIECKMANN LEI 12.737/2012

O princípio da legalidade contém dois princípios contidos de forma implícita. O primeiro deles é o princípio da Reserva Legal através deste entende-se que um ato criminal só pode ser definido por lei e esta lei é em um sentido mais estrito, ou seja, um ato legislativo vai dizer se um determinado ato cometido por uma pessoa é ou não crime, portanto pela reserva legal não pode existir crime ou não pode ser definido com crimes atos através de medida provisória ou decreto.

O segundo princípio que está implícito no princípio da legalidade é o princípio da anterioridade da lei penal, através deste vemos que um ato criminoso só é considerado desta forma a partir do momento que que a lei esteja vigorando. Há uma exceção ao princípio da anterioridade, que é quando já existe uma lei que defini como crime um determinado ato e uma lei posterior vez e reduz ou ainda de outra forma beneficia no aspecto da pena aquele agente.

Em março de 2012, atriz Carolina Dieckmann teve seu computador invadido após ter sido vítima de fraude virtual ao abrir um e-mail em que acreditava ser de fonte segura. Fotos íntimas da atriz foram copiadas do seu equipamento e posteriormente Carolina começou a receber ameaças de extorsão.

A atriz se engajou nesta causa de punibilidade deste tipo de delito e a lei 12.737/2012 passou a ter o seu nome.

Esta lei já vinha tramitando no Congresso através do projeto 2.973/2011. Com o interesse de Carolina por esse projeto, o mesmo ganhou força e teve seu processo mais acelerado tornando-se lei em 30 de novembro de 2012, tendo como objetivo tipificar os crimes informáticos, pois até então não havia lei específica para esse tipo de crime o que levava os agentes anteriormente a serem tipificados por outros crimes do código penal.

A lei 12.737/2012 alterou o código penal, acrescentando os artigos 154A e 154B. Os crimes tipificados pela Lei Carolina Dieckmann são os crimes cometidos contra os dispositivos informáticos da vítima e não com o computador do meliante.

Analisando o artigo 154A, dois pontos devem ter atenção especial. No primeiro o importante a ser destacado é que tem que haver uma violação indevida de dispositivo de segurança para caracterização do delito neste artigo, pois se neste equipamento não houver um dispositivo de segurança instalado como um antivírus, firewall ou mesmo uma senha, ou ainda se não houver esse tipo de programa ativo no equipamento em questão, não se poderá falar em invasão e violação indevida que é característica deste crime. As informações seriam acessadas de forma indevida, contudo não estaria tipificada nesta lei. Um agente criminoso que acessa um equipamento que não tem um dispositivo de segurança não violando senhas, firewall ou qualquer outro tipo de programa do gênero, este não cometeu o crime de invasão ou outro delito informático previsto nesta lei.

O segundo ponto e não menos importante seria no que diz respeito a parte do artigo 154A que diz "...autorização expressa ou tácita do titular..." Ao enviar um equipamento para manutenção para uma empresa que realiza esse tipo de serviço o usuário está autorizando tacitamente. Caso ocorra em hipótese uma adulteração, destruição de dados ou informações o agente causador não teria seu crime tipificado neste artigo.

O código Penal em seus artigos 154 e 154A versam:

> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com 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 três meses a um ano, ou multa.
> Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime e cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

6.2 MARCO REGULATÓRIO DA INTERNET

Criado através do Projeto de lei 2.126 de 2001, teve por base o Princípio da Governança e do uso da Internet, que reconhecia que o acesso à internet é essencial

ao exercício da cidadania. O plenário da Câmara dos Deputados aprovou o projeto em março de 2014 transformado na Lei ordinária de 12.765/14 que versa:

> **Art. 1º** Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria

A lei do Marco Civil tem com intenção proteger a privacidade do usuário na internet buscando assegurar a inviolabilidade e o sigilo das comunicações conforme determina a CR/88 em seu artigo 5º inciso X.

> 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:
> X - 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;

Nota-se que a Lei do Marco Civil nos dispositivos abaixo colacionados:

> **Art. 3º** A disciplina do uso da internet no Brasil tem os seguintes princípios:
> (...)
> II - proteção da **privacidade**;
> **Art. 8º** A garantia do direito à **privacidade** e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.
>
> **Art. 11º** Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à **privacidade**, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
> (...)
> § 3o Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à **privacidade** e ao sigilo de comunicações.

A Lei assim determina que provedores não podem violar ou o direito à intimidade e vida privada dos usuários, ou seja, não pode haver monitoração dos dados trafegados pela rede ou efetuar a divulgação destes, contudo esse fato pode ocorrer caso haja ordem judicial. Outro ponto a se destacar é que a exclusão dos dados deve ser garantida quando as partes encerrarem as relações.

A recente norma tem como obrigação de proteger a atual sociedade informacional, embora a internet tenha se popularizado no Brasil na década de 1990 é louvável o papel do Marco Civil da Internet o direito à privacidade de forma essencial.

Um exemplo recente onde o Marco civil da internet foi aplicado foi o caso do cantor Cristiano Araújo falecido em 2015 em um acidente de trânsito, tendo material informático relacionado ao fato divulgado na internet, mas no meio jurídico o fato de maior relevância foi o vídeo do corpo do cantor sendo preparado paro o funeral, evento compartilhado por dois funcionários da empresa que prestava serviço funeral a família.

Devido ao indiscriminado compartilhamento deste material pela internet, principalmente pelo aplicativo de mensagens instantâneas *"whatsapp",* aplicou-se a lei 12.965/2014 em seus artigos 10 e 11 que trazem:

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

É notório que, no caso relatado do cantor, a disponibilização de material informático de seu cadáver, feriu a honra e vida privada.

O Código Penal em relação ao mesmo crime também tipifica em seu artigo 212 mais um crime em relação ao falecimento do cantor, o crime de Vilipêndio.

> Art. 212 - Vilipendiar cadáver ou suas cinzas.
> Pena - detenção, de um a três anos, e multa.

Nesta breve analise da Lei 12.765/14, conclui-se que a privacidade, a honra e imagem pessoal dos usuários da internet devem receber cuidados e estes têm que permanecer protegidos. É mais essencial a regulamentar a internet hoje do que na

década de 1990 e mais necessário no futuro do que hoje, é por isso que o ordenamento jurídico evolui em conjunto com o comportamento da sociedade.

7 LEGISLAÇÃO INTERNACIONAL PARA CRIMES DE INFORMÁTICA

Em 2001, o Conselho da Europa aprovou a convenção de Budapeste sobre o Cibercrime. Referente a crimes efetuados pela internet essa é uma referência legislativa mundial, tanto que fora assinada por 43 países e ratificada por 21 nações signatárias. O Brasil não assinou o tratado, ao contrário de Estados Unidos, Canadá, Japão, França e Espanha, por exemplo.

Foi determinado nesta, Convenção, procedimentos de investigação nesta convenção, obrigando fornecedores de serviços informáticos a conservar imediatamente os dados de tráfego, e estas deverão comunicar às autoridades investigadoras dados informáticos necessários para identificação do criminoso.

Em 2007, a BSA The Software Alliance, empresa americana de desenvolvimento de software e a Gigante em produção de software de segurança Symantec unidas a outras empresas de tecnologia pressionavam o congresso dos EUA para o combate a crimes virtuais.

Em 2016, conforme pesquisa da BSA o Brasil atingia 47% utilização de softwares piratas, ou seja softwares não licenciados. No mesmo relatório a BSA diz que empresas podem minimizar riscos à segurança com a aquisição de softwares por meios legais.

Poucos são os países que tem legislação específica para crimes virtuais, contudo a maioria dos crimes é cometido fora das fronteiras dos países cujo criminoso reside. O direito internacional orienta que primeiramente o acusado seja processado em seu país o que se torna na maioria das vezes impossível devido à ausência de leis específicas que definam na natureza penal. Outro fato é que se o crime atinge outro país o criminoso deveria ser extraditado, de acordo com a forma legal daquele país tendo que ser verificado assim os tratados de extradição. Assim sendo, inexiste na maioria das vezes punição contra crimes virtuais além das fronteiras, o que serve de incentivo a prática criminosa em vários lugares do mundo.

Diante o exposto, a aplicação do princípio da universalidade ou cosmopolita, seria o mais eficaz pois esse princípio diz que a lei penal aplica-se a qualquer um e em todo lugar, contudo para sua aplicabilidade haveria de ter cooperação entre os países com tratados e convenções internacionais referentes a crimes virtuais. Deve-se considerar que é um mal universal e o interesse de tolher é de qualquer Estado.

7.1 BRASIL SOB PRESSÃO

Mediante reclamações do Japão e União Europeia, entregues em 2012, à OMC, Organização Mundial do Comércio, em novembro de 2016, entende que os incentivos fiscais conferidos aos setores de informática e telecomunicações no Brasil conforme determina a Lei 8.248 de 23 de outubro de 1991 Lei de Informática, seriam indevidos, considerados como subsídios ilegais na decisão do Painel que verificou os casos, de conforme o relatório final obtido pela agência de notícias Reuters.

A lei, devido ao seu benefício, proporcionou ao Brasil a criação de várias empresas, gerando assim mais de cem mil empregos e faturamento em torno de US$ 10 bilhões, fora os investimentos em inovação e pesquisa e desenvolvimento.

No dia 30 de agosto de 2017, a Organização Mundial do Comércio estabeleceu ao Brasil um prazo de somente 90 dias para alteração da lei vigente. O Brasil apresentou recurso que será avaliado.

A P&D Brasil representa empresas desenvolvedoras de tecnologia no país apresentou uma alegação propondo a troca de subsídios da redução do IPI por créditos tributários tendo por base a quantidade de investimentos em desenvolvimento e pesquisas.

Pela importância estratégica, a lei 8.248 deve ser mantida mais uma vez revisada e atualizada e a soberania nacional externa respeitada a lei de informática é muito importante para o desenvolvimento do país e deve acompanhar o que de novo ocorre no mundo, pois o direito se adequa conforme as mudanças sociais.

8 DIFICULDADE DE OBTENÇÃO DE PROVAS NO MEIO ELETRÔNICO

Investigação criminal são empenhos iniciais devidamente dentro da lei buscam apurar a materialidade, existência, autoria e circunstância de uma ação penal coletando elementos de informação que poderão ser ou não utilizadas em um processo criminal.

O ordenamento jurídico brasileiro não proíbe a utilização de provas eletrônicas conforme o código civil que diz em seu artigo 225:

> 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.

Ademais o Código De Processo Civil de 2015 versa que:

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

Um usuário, quando utiliza a rede mundial de computadores, através de um equipamento informático, recebe uma identificação virtual o *internet Protocol* que é chamada também chamado de IP.

Este IP é o principal protocolo de comunicação da internet, este é o responsável por encaminhar e endereçar os pacotes de dados que trafegam na internet. O IP é disponibilizado ao usuário através de um provedor de acesso que o fornece juntamente com a data, hora e o fuso horário do sistema. Estes elementos são fundamentais para a verificação de sigilo de dados. É através do provedor de acesso à internet que após determinação judicial pode verificar o sigilo de dados informáticos vincule o endereço IP distribuído ao usuário naquela data e hora em que ocorreu o crime, ao seu endereço físico.

Se tratando de crimes praticados pela internet, são várias as dificuldades de investigação como elenca o advogado especialista em crimes virtuais BURG entrevistado pela revista jurídica CONJUR (Consultor Jurídico) que diz:

> A internet facilita a impunidade, uma vez que a investigação é mais complicada e, muitas vezes, quando é identificado o autor, já ocorreu a prescrição. Isso sem contar na questão da fronteira: o crime pode ser cometido por alguém que está em outro país, com leis completamente diferentes.
> A fronteira acaba motivando também, de certa forma, a impunidade. E aqui, infelizmente, não tem muito o que fazer. Porque não tem como criar uma lei obrigando o cidadão da Estônia a vir para o Brasil no prazo. [Disponível em https://www.conjur.com.br/2017-fev-05/entrevista-daniel-burg-especialista-crimes-virtuais, acessado em 03 de nov. 2017]

BURG enfatiza que:

> A legislação brasileira não está adequada e, muitas vezes, o crime prescreve sem que haja um avanço significativo nas investigações. Nos crimes contra a honra, por exemplo, há uma enorme dificuldade para se identificar o autor de ofensas realizadas na internet, e sem a identificação sequer é possível oferecer queixa-crime. [Disponível em https://www.conjur.com.br/2017-fev-05/entrevista-daniel-burg-especialista-crimes-virtuais, acessado em 03 de nov. 2017]

André Zonaro Giachetta em contraposto ao descrito acima diz que:

> É muito mais fácil identificar crimes pela internet, que deixam pegadas, do que muitos crimes no mundo físico. O meio digital possibilita muito mais a identificação e provas do que antes e, mais do que se imagina, é possível chegar ao verdadeiro autor do ato. Em São Paulo, temos a Lei 12.228/06, que disciplina a obrigatoriedade da guarda dos registros dos dados cadastrais dos usuários de conexão à rede mundial de computadores em *lan houses* e *cybercafés* por 60 meses [Disponível em https://www.conjur.com.br/2009-jul-25/identificar-autores-crimes-eletronicos-cada-vez-possivel Acessado em 03 de nov. 2017]

Giachetta ainda afirma que:

> Há graus de dificuldade para indicar o culpado, mas não é impossível." Para ele, o número do IP hoje é muito mais relevante do que qualquer outro dado do internauta. “Em um crime de internet, ter o RG do suspeito é menos importante do que o endereço de IP, que prova o momento e local em que o ato foi cometido.” [Disponível em https://www.conjur.com.br/2009-jul-25/identificar-autores-crimes-eletronicos-cada-vez-possivel Acessado em 03 de nov. 2017]

O rastreamento de IP não é a melhor maneira de se localizar um criminoso virtual, no entanto a única forma de controle para barrar o aumento da criminalidade virtual é o Direito, pois esse de forma coercitiva puni as condutas ilícitas e detém o caratê imperativo através de leis. Entretanto faz-se necessário um estudo aprofundado sobre

a rede mundial de computadores e sua evolução suas mudanças presumíveis e seus delitos, deixando assim de existir normas menos eficazes.

O Estado não pode permitir que atos delituosos venham ferir bens jurídicos tutelados, este deve oferecer uma restituição da ordem social evitando assim o aumento da criminalidade virtual e ao mesmo acompanhando a evolução a internet.

CONSIDERAÇÕES FINAIS

O principal objetivo da presente monografia foi explorar sob a ótica da legislação Brasileira os crimes virtuais, contudo facilmente constatamos a dificuldade de delinear o espaço virtual e suas fronteiras.

Constata-se também a falta capacitação e conhecimento específico por parte de investigadores, legisladores e por fim das autoridades legais, para assim conseguir identificar, criar leis mais objetivas e punir os criminosos virtuais.

A sociedade de forma geral necessita de informações legais sobre os procedimentos de utilização da internet e os limites desta. O direito deve se apresentar de forma equivalente a velocidade de evolução da rede mundial de computadores.

A atualização constante do nosso ordenamento jurídico, somado aos mecanismos de prevenção e por último os de repressão nos mostraram que a criação de um direito específico não se faz necessário, mas sim uma tipificação mais objetiva e específica para tratar tais delitos.

Bens jurídicos tutelados pelo Estado não podem ser feridos, portanto o Estado não pode permitir que isso ocorra, para tanto o Estado deve restituir sempre que necessário a ordem social, acompanhar a evolução da internet e evitar de forma completa que continue a aumentar os crimes virtuais.

A constituição da prova é elemento importante para o ordenamento jurídico, averiguando se ocorreu, quando ocorreu e como foi a prática do delito

Conforme argumentos apresentados algumas características dos crimes virtuais o processo de investigação e consecutivamente a tipificação penal.

Portanto, faz-se necessário repensar em aplicação de penas brandas tais com a lei 12.737, pois o ordenamento jurídico brasileiro possibilita a modificação das penas até quatro anos, o que frente aos crimes virtuais aumenta a sensação de impunidade.

Em suma, a criação de penas mais severas, leis penais mais positivas e melhor fundamentadas, realçaria a função do direito penal que versa sobre a proteção de bens jurídicos essenciais, promovendo essa proteção integralmente e de forma mais eficaz contra os crimes virtuais.

Por fim, e não menos considerável, é importante denunciar os crimes virtuais, hoje já é possível fazer uma denúncia através da própria internet. O Ministério Público Federal, através de seu site, oferece a ferramenta “Digidenuncia” que ao acessá-la o usuário pode optar em se identificar ou não. Também algumas cidades as denúncias podem ser feitas pessoalmente em delegacias especializadas em Crimes Cibernéticos, estas cidades podem ser pesquisadas no site do Instituto de Defesa Cibernética. Outra Forma de efetuar uma denúncia é através da “SaferNet” que é um órgão internacional que trabalha contra os crimes virtuais. Muitos delitos acabam se repetindo por falta de denúncia.

REFERÊNCIAS

ARAS, Vladimir. **Crimes de informática. Uma nova criminalidade**. Jus Navigandi, Teresina, ano 5, p. 51, out. 2001. Disponível em: <https:// jus.com.br/artigos/2250/crimes-de-informatica>. Acesso em: 10 out. 2017.

BRASIL. Supremo Tribunal Federal – Recurso de Habeas Corpus n. 76.689-0 – Pernambuco – Primeira Turma – Relator: Ministro Sepúlveda Pertence, DJU de 6.11.1998, p.03

CARVALHO, Ana Paula Gambogi. **Contratos Via Internet. Belo Horizonte**: Del Rey, 2001.

CERT.BR - **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**. Disponível em: .Acesso em: 31 out. 2017.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.p.48

FRAGOSO, Heleno Cláudio. **Lições de direito penal: parte especial**: arts. 121 a 212 do CP.Rio de Janeiro: Forense, 1983.p.5

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

GROSSI, Bernardo Menicucci. **Proteção jurídica do Software**. Belo Horizonte: Mandamentos, 2005

FERREIRA, Aurélio Buarque de Holanda. **Novo dicionário da língua portuguesa. 2ª Ed. Rio de Janeiro**: Nova Fronteira, 2000.p.1016

http://advivo.com.br/blog/luiz-claudio-tonchis/redes-sociais-privacidade-perfis-fake-e-crimes-virtuais Acesso em 04 de nov. 2017

https://abimaelborges.jusbrasil.com.br/artigos/111823710/lei-carolina-dieckmann-lei-n-12737-12-art-154-a-do-codigo-penal Acesso em 04 de nov. 2017

http://g1.globo.com/rio-de-janeiro/noticia/2012/05/suspeitos-do-roubo-das-fotos-de-carolina-dieckmann-sao-descobertos.html Acesso em 02 de nov. 2017

http://idciber.eb.mil.br/index.php?option=com_content&view=article&id=793:onde-denunciar-crimes-virtuais-lista-de-delegacias-especializadas&catid=78&Itemid=301 Acesso em 03 de nov. 2017

http://portal.imprensanacional.gov.br/ Acesso em 03 de nov. 2017

https://suzannamacedo.jusbrasil.com.br/artigos/215684309/analise-critica-da-lei-do-marco-civil-da-internet-lei-12965-2014-e-anteprojeto-de-lei-de-protecao-de-dados-pessoais. Acesso em 03 de nov. 2017

https://vicentemaggio.jusbrasil.com.br/artigos/121942478/novo-crime-invasao-de-dispositivo-informatico-cp-art-154-a Acesso em 03 de nov. 2017

http://www.bsa.org/?sc_lang=pt-BR. Acesso em 03 de nov. 2017

https:// www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1449738, Acesso em: 01 nov. 2017

http://www.cnj.jus.br/atos-normativos?documento=181 Acesso em 03 de nov. 2017

https://www.conjur.com.br/2009-jul-25/identificar-autores-crimes-eletronicos-cada-vez-possivel Acesso em 03 de nov. 2017

https://www.conjur.com.br/2013-fev-04/eduardo-cabette-crime-invasao-dispositivo-informatico Acesso em 03 de nov. 2017

https://www.dgti.ufla.br/site/lei-de-crimes-informaticos/ Acesso em 04 de nov. 2017

http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm Acesso em 04 de nov. 2017
http://www.planalto.gov.br/ccivil_03/leis/L8248.htm Acesso em 03 de nov. de 2017

http://www.planalto.gov.br/ccivil_03/leis/LEIS_2001/L10176.htm Acesso em 03 de nov. 2017

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l13023.htm. Acesso em 03 de nov.2017

http://www.planalto.gov.br/ccivil_03/leis/2002/L10408.htm. Acesso em 03 de nov. 2017

http://www.rogeriogreco.com.br/?p=2183 Acesso em 03 de nov. 2017

http://www2.camara.leg.br/camaranoticias/noticias/CIENCIA-E-TECNOLOGIA/199806-SAIBA-COMO-OS-CRIMES-NA-INTERNET-SAO-TRATADOS-EM-OUTROS-PAISES.html. Acesso em 03 de nov.2017

https://www12.senado.leg.br/noticias/materias/2013/09/03/entenda-o-projeto-de-marco-civil-da-internet Acesso em 03 de nov. 2017

INELLAS, Gabriel Cesar Zaccaria de. Crimes na Internet. São Paulo: Editora Juarez de Oliveira, 2004. p.51

PINHEIRO, Patrícia Peck. Direito Digital. 4. Ed. São Paulo: Saraiva, 2010.p.65.

ROHRMANN, Carlos Alberto. Curso de Direito Virtual. Belo Horizonte: Del Rey, 2005.

VADE MECUM. 24ª Ed. São Paulo. Saraiva, 2017.