FACULDADE DE DIREITO DE IPATINGA
CURSO DE DIREITO

MANOEL HENRIQUE PEREIRA TORRES

CRIMES VIRTUAIS

Ipatinga
2020

MANOEL HENRIQUE PEREIRA TORRES

CRIMES VIRTUAIS

Monografia apresentada como requisito parcial para obtenção do grau de Bacharel em Direito, da Faculdade de Direito de Ipatinga.

Orientador: Prof. Ms. Breno Inácio da Silva.

Ipatinga

2020

Dedico esta monografia a TODAS as pessoas que me apoiaram durante minha jornada acadêmica. Agradeço à Deus pelas oportunidades que me foram dadas no decorrer da vida. Aos meus professores e orientador pelo companheirismo na elaboração deste projeto de pesquisa.

AGRADECIMENTOS

Agradeço primeiramente aos meus queridos pais, por todo o esforço desmedido empregado para a minha criação e amadurecimento, resultando na conclusão dessa fase da minha vida, e por todo o amor, carinho e paciência que dedicaram durante todos esses anos de estudo.

A toda equipe de professores e colaboradores da Faculdade de Direito de Ipatinga, que sempre tiveram muito carinho comigo e me ajudaram no desenvolver deste trabalho.

Por fim, agradeço a todos que de algum modo, contribuíram na minha formação, e principalmente aos meus colegas de sala, que tive a oportunidade de conhecer na graduação e que permaneceram do meu lado durante essa trajetória.

“*Uma vez que se privou o homem da verdade, é pura ilusão pretender torná-lo livre. Verdade e liberdade, com efeito, ou caminham juntas, ou juntas miseravelmente perecem”. (Papa João Paulo II)*

RESUMO

No presente trabalho, serão abordados sobre o conceito de crimes cibernéticos, apontando a tipificação dos crimes, bem como algumas noções gerais de cibercriminalidade, esclarecendo sobre as categorias de crimes virtuais. Será abordado também como a investigação policial é fundamental para este tipo de crime. Assim, o enfoque da presente pesquisa é um estudo sobre o exercício do direito à liberdade de expressão, a fim de se determinar os limites ao exercício desse direito na internet, bem como as repercussões dos ataques à honra e à imagem de um indivíduo através desse meio de comunicação que vem constrangendo muitas pessoas na atualidade.

Palavras-Chave: Cibercriminalidade. Liberdade. Investigação.

SUMÁRIO

1 INTRODUÇÃO

O presente trabalho teve por objetivo analisar sobre os denominados crimes virtuais, bem como compreendendo quais condições a legislação brasileira atua em relação a este tipo de prática delituosa. Será abordado os tipos de crimes virtuais, desde sua concepção até sua disseminação na sociedade atual, através da realização de pesquisa bibliográfica e análises de casos de crimes cibernéticos no Brasil.

É imprescindível o estudo do conceito de cibercriminalidade e liberdade de expressão, esclarecendo sobre a livre manifestação de pensamento vedando o anonimato, ou seja, qualquer pessoa tem o direito de expressar suas opiniões desde que se identifique como responsável pelas mesmas.

Os crimes virtuais ocorrem desde antes o surgimento da internet, trazendo consigo uma nova forma de interação social, mas apesar de se destacar pelas inovações positivas, o lado obscuro, em se tratando de caráter criminal (cibercrimes), ocasionado por este desenvolvimento tecnológico tem destacado negativamente. É uma situação muito preocupante, pois tem se justificado por grande parte dos usuários, a realização de determinados atos como exercício do direito a liberdade de expressão, direito este que deve ser utilizado dentro dos parâmetros legais.

Assim, buscou-se analisar alguns dos crimes virtuais e a forma de como se proteger desta nova e atual modalidade de crime. A internet já invadiu praticamente todos os nossos atos cotidianos da vida, influenciando na maneira que vivemos hoje que nada mais é que um mundo necessitado de informação.

Será analisado também de onde se originou a denominação “crimes virtuais” e, com isso, delimitar até onde vão esses crimes. Com isso, foram estudadas as formas pelas quais as leis penais se direcionam a este tipo de crime e mostrar que ainda há pouca atenção para a referida situação.

Por fim, a motivação para a realização deste trabalho esta amplamente direcionada em auxiliar futuras pesquisas acadêmicas, tornando o mesmo uma rica fonte de pesquisa. Vale ressaltar que, ainda não há tipificação própria para todas as modalidades de crimes praticados virtualmente, em alguns casos, somente algumas leis em caráter *latu sensu* vêm sendo utilizadas como solução para tais determinados crimes.

2 CONCEITO DE INTERNET E CRIMES VIRTUAIS

Pode-se dizer que a internet consiste em uma rede mundial de computadores e demais dispositivos eletrônicos conectados entre si, que possui como principal objetivo o compartilhamento de informações. Tais informações são transferidas juntamente com um protocolo de internet, que funciona como um código de rastreamento postal, denominado na língua inglesa como *Internet Protocol*, assim esclarece Gabriel Inellas:

> A definição do conceito de internet pode ser apresentada como uma rede de computadores interligada a uma rede de menor porte que se comunica entre si, utilizando um endereço "lógico" chamado de endereço IP, onde diversas informações são trocadas, surgindo daí um problema, pois existe uma infinidade de informações pessoais disponíveis na rede, ficando à disposição de milhares de pessoas que possuem acesso à internet, e quando não são disponibilizadas pelo próprio usuário, são procuradas por outros usuários que buscam na rede o objetivo única e exclusivamente de cometer crimes, os denominados Crimes Virtuais [...]. (INELLAS, 2004, p. 3).

As primeiras aparições destes crimes datam do século passado, por volta da década de 1970, sendo que, em grande parte das ocorrências os infratores eram pessoas com amplo saber no ramo informático, que utilizavam de seus conhecimentos para invadirem sistemas de segurança de grandes empresas. (NUNES, 2015).

> Os primeiros crimes de informática iniciaram-se na década de 70, sendo executados em sua grande maioria por pessoas especializadas no ramo informático com o objetivo principal de adentrar ao sistema de segurança das grandes empresas tendo como maior foco as denominadas como instituições financeiras. O perfil atual dos criminosos que atuam nessa área foi alterado, já que nos dias atuais qualquer pessoa que tenha um conhecimento, porém não tão aprofundado basta ter acesso a rede mundial de computadores para que consiga lograr êxito na execução de um crime virtual. (CASTRO, 2003, p.9).

Os crimes virtuais são todas as atividades criminosas realizadas por meio de computadores ou através da internet. Para a prática destes crimes podem ser empregados diversos métodos e ferramentas, tais como phishing, vírus, spyware, ransomware e engenharia social, geralmente visando a subtração de dados pessoais. Tais atividades vão muito além da obtenção de dados, segundo conceitua Patrícia Pinheiro:

> Podemos conceituar os crimes virtuais como sendo as condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas, a interceptação de comunicações, modificações de dados, infrações os direitos de autor, incitação ao ódio e descriminação, chacota religiosa, transmissão de pornografia infantil, terrorismo, entre diversas outras formas existentes. (PINHEIRO, 2010, p. 46).

De fato, a origem do conceito de crime virtual esta inteiramente ligada ao acesso ilegal de sistemas de informação, que ocasionam grandes transtornos a seus titulares, mas não há um consenso geral de como denomina-los. Por conta disso, é importante que se observe o bem jurídico tutelado, e se o crime praticado configura-se na mesma categoria, para então aplicar o tipo penal correspondente. Diante da diversidade de pensamentos doutrinários em referência à classificação dos crimes virtuais, Ivette Senise Ferreira sugere de forma resumida a seguinte classificação desses crimes. (CARNEIRO, 2012).

> Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial. (FERREIRA, 2005, p. 261).

São diversas as classificações doutrinárias e discussões referentes ao tema abordado, mas considerando o papel desempenhado pelo computador no contexto da prática do ato ilícito, pode-se dividir os crimes virtuais em duas categorias, como sendo próprios e impróprios. (TATEOKI, 2016).

2.1 Tipificação dos crimes virtuais

Inicialmente, os crimes virtuais são considerados como um crime de meio, ou seja, praticados virtualmente. Portanto, não se trata de um crime fim por natureza, pois essa modalidade só ocorre em ambiente virtual, com a ressalva dos crimes cometidos por *hackers*, em que de alguma forma existe a probabilidade de serem enquadrados na tipificação com equivalência a estelionato, extorsão, falsidade ideológica, fraude e diversos outros equiparados. Desta feita pode-se mencionar que o elemento de materialização do comportamento criminoso pode ser virtual; todavia, em algumas ocorrências, o crime não. (NUNES, 2015, p.14).

Para explanar este fluxo de teoria, expomos como exemplo o julgamento pelo ex presidente e ministro Sepúlveda Pertence, do Supremo Tribunal Federal, do habeas corpus (76689/PB), de 22 de setembro de 1998, sobre crime de computador. (NUNES, 2015).

EMENTA: "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: HC 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 norma 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 criminada, o meio técnico empregado para realiza- lá 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 pende de informações técnicas de telemática que ainda pairam acima do conhecimento do homem comum. (SEPÚLVEDA, 1998, p. 3).

Percebe-se que grande parte dos crimes informáticos coincide igualmente no mundo físico e, por conta da dificuldade em identificar os infratores e pela falta de jurisdição para julgamento destes crimes, ocasionalmente a tipificação em caráter mais específico, *stricto sensu,* fica prejudicada. Entretanto, aplica-se o princípio da territorialidade em solução a este conflito de competência originado pela escassez de legislação mais célere e atualizada. O infrator que praticou determinado crime informático deverá ser julgado dentro dos parâmetros da legislação vigente no Código Penal de forma residual, sempre que houver ausência de norma específica. Tem-se como exemplo a aplicação da lei penal em relação ao crime de furto praticado na modalidade virtual. (CARNEIRO, 2012).

> Um crime que ocorre diariamente é denominado como furto de dados, onde é tipificado pelo Código Penal como furto em seu Art. 155 consistindo em “subtrair, para si ou para outrem, coisa alheia móvel”, o ponto que se tem arrazoado, é se poderia enquadrar o furto de dados como sendo o furto do

> art. 155 do CP, já que o mesmo poderia não se enquadrar no tipo legal, de modo que na conduta do agente o mesmo pode alterar os dados da empresa e em sequência extinguir, ou também pode leva-los por via de cópia e não eliminá-los, porém neste caso não haveria o quesito de indisponibilidade do bem, no caso para configurar a subtração. (PINHEIRO, 2010, p. 313).

Dentre os diversos crimes informáticos conhecidos, destacam-se os mais comumente ocorridos em território brasileiro, assim exposto em seguida:

> **a)** Pirataria: Copiar dados em CDs, DVDs ou qualquer base de dados sem prévia autorização do autor é percebido como pirataria em conformidade com a Lei 9.610/98. De acordo com o art. 87 da referida lei, "o titular do direito patrimonial sobre uma base de dados terá o direito exclusivo, a respeito da forma de expressão da estrutura da mencionada base". As penas possuem uma variação de 2 meses a 4 anos, podendo haver aplicação ou não de multa, a estar sujeito se houve reprodução parcial ou total, venda ou disponibilização ao público via cabo ou fibra óptica;
>
> **b)** Dano ao patrimônio: Previsto no art. 163 do Código Penal. O dano pode ser simples ou qualificado, sendo estimado qualificado quando "o dano for contra o patrimônio da União, do Estado, do Município, de empresa concessionária de serviços públicos ou de sociedade de economia mista". Nota-se que para ser qualificado, o objeto do dano deverá ser da União, do Estado, do Município, de empresa concessionária de serviços públicos ou de sociedade de economia mista, podendo ser aplicado, por exemplo, àqueles crimes de sabotagem dentro de repartições públicas. A mesma lógica é utilizada quando se trata de vírus, por ser considerado como tentativa (perante comprovação) de dano. A punição para dano simples é de detenção, de um a seis meses, ou multa. Já para dano qualificado, a pena prevista é detenção de seis meses a três anos e multa;
>
> **c)** Sabotagem informática: A sabotagem, no tocante aos termos econômicos e comerciais, será a invasão de determinado estabelecimento, objetivando prejudicar e/ou roubar dados. Segundo Milton Jordão, "versa a sabotagem informática no acesso a sistemas informáticos visando a extinguir, total ou parcialmente, o material logo lá contido, podendo ser cometida por meio de programas destrutivos ou vírus". A lei apenas prevê punição de 1 a 3 anos de prisão e multa, porém não inclui a sabotagem informática em seu texto;
>
> **d)** Pornografia infantil: O art. 241 do ECA (Estatuto da Criança e do Adolescente) veda "apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, de modo inclusivo na rede mundial de computadores ou Internet, fotografias ou imagens com pornografia ou cenas de sexo explícito abrangendo criança ou adolescente". Esse tipo de conduta é denominado como exclusivamente crime virtual, pois ele só ocorre única e exclusivamente através do uso da internet. A punição para quem contravenha este artigo do estatuto é de detenção de 2 a 6 anos e multa;

e) Apropriação indébita: O Código Penal faz referência apenas à apropriação indébita de bens materiais, como por exemplo CPU, mouse e monitor, sendo afastada a forma de apropriação de informações. Não obstante, se a apropriação ocorrer através de cópia de software ou de informações que legalmente concernem a uma instituição, podem-se aplicar punições por pirataria. A pena para apropriação indébita está prevista no artigo 168 do referido código, sendo de reclusão de 3 a 6 anos e multa para quem praticar ato fraudulento em benefício próprio;

f) Estelionato: Nesta tipificação de crime, o Código Penal pode ser aplicado de acordo com o seu artigo 171, de forma que o crime tenha sido executado plenamente. Segundo Da Costa, o estelionato "consuma-se pelo alcance da vantagem ilícita, em prejuízo alheio. É também admissível, na forma tentada, na sua amplitude conceitual, porém é de ser buscado o meio utilizado pelo agente, uma vez que impunível o meio inidôneo". A pena é de reclusão de 1 a 5 anos e multa;

g) Divulgação de segredo: O Código Penal nada menciona em referência caso o segredo seja revelado via computador, sendo tratado da mesma forma que se fosse divulgado por documento, por se tratar de uma forma de correspondência;

h) Crimes contra a liberdade individual: São os tipificados no Código Penal como crimes de ameaça (artigo 147), de inviolabilidade de correspondência (artigos 151 e 152), de divulgação de segredos (artigos 153 e 154) e de divulgação de segredos contidos ou não em sistemas de informação ou bancos de dados da Administração Pública (artigo 153, § 1º-A). O crime de interceptação telefônica e de dados, que tem como bem jurídico tutelado os dados, pois o que se tem como objetivo é proteger a transmissão de dados e restringir o uso dessas informações para fins fraudulentos. O tipo penal citado protege igualmente o tema da inviolabilidade das correspondências eletrônicas, o que já é garantido na própria Magna Carta(Constituição Federal de 1988), no seu artigo 5º, XII, assim como ocorre a sua remissão ao paragrafo art. 1º, parágrafo único da Lei nº 9.296, de 24 de julho de 1996, onde regula o inciso XII, parte final já citado. XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal. Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça. Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.

i) Difamação, injúria e calúnia: São os crimes de calúnia (artigo 138), de difamação (artigo 139) e de injúria (artigo 140). Os criminosos são estimulados pelo quesito do anonimato, podendo ocorrer em locais virtuais tais como chats, blogs, pelo envio de spams e por meio de publicações em homepages, entre outros meios de postagem eletrônica. Outro exemplo a ser citado que pode acontecer nas redes sociais, é se alguém divulgar informações falsas que lesem a reputação de outra pessoa ofenda a dignidade do outro ou de má-fé acusem alguém de criminoso, desonesto ou perigoso;

j) Falsa identidade: Sucede quando alguém apresenta nome ou dado diverso do qual consta em seu documento de identificação, tais como idade, estado civil, sexo e outras características com o desiderato de conseguir alguma vantagem ou prejudicar outra pessoa. O crime do artigo 151 do CP, denominado como crime de violação de correspondência, é um tipo

> inteiramente aplicável à conduta de interceptação e violação de e-mails, pois os tipos previstos na Lei 6.538/78 são inaplicáveis, pois essa dispõe sobre os serviços postais explorados pela União, por meio de empresa pública vinculada ao Ministério das Comunicações. Neste tipo, o bem jurídico tutelado é a integridade dos Serviços Postal e de Telegrama nacionais, devendo a correspondência se dar por meio da via postal ou por telegrama, proposições nas quais o e-mail não se encaixa. (OLIVEIRA, 2002, p. 73).

As modalidades expostas acima mostram a quão ultrapassada é a legislação sobre crimes informáticos atualmente. Com o passar dos anos esses crimes evoluíram de forma considerável, diferentemente quanto às formas de prevenção e em relação própria legislação, que ainda tem dificuldade em sua aplicabilidade. Isso faz com que os infratores na maioria dos casos, obtenham sucesso em suas atividades ilícitas.

Uma modalidade que vem se tornando muito comum é o envio de e-mails falsos simulando serem originados de órgãos estatais, instituições financeiras e empresas de telecomunicação, como por exemplo: a Receita Federal, Serasa, BV Financeira, etc... Essa prática tem como objetivo enganar o registrado do e-mail com uma mensagem, por meio de um falso link, declarando a existência de suposta pendência financeira.

Acessado o link, o usuário é redirecionado para uma página onde um programa mal intencionado é instalado. O criminoso a partir deste começa a recolher dados e qualquer tipo de informação que lhe seja útil.

Há crimes cujo intuito é demonstrar a fragilidade de sistemas, como é o caso das invasões a sites e aplicativos de relacionamento e interação social, como *Tinder*, *Facebook* e *Instagram.* Existe uma infinidade de crimes virtuais, muitos ainda nem possuem um *modus operandi* conhecido e outros ainda nem foram descobertos. (BLUM, 2004).

2.2 Crimes virtuais próprios

Entende-se como crimes virtuais próprios ou puros, sendo aqueles em que o agente se utiliza necessariamente do computador para a prática de atos ilícitos, no qual este, como meio tecnológico, é usado como principal instrumento para execução do crime. Essa categoria caracteriza-se não só pela invasão de dados não

autorizados, mas por toda interferência em dados informatizados como, por exemplo, invasão de dados armazenados em computador, seja no intuito de modificar, alterar, inserir dados falsos, ou seja, que atinjam diretamente o *software* ou *hardware* do computador visando prejudicar servidores e sistemas.

Para Damásio de Jesus:

> Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado. (DAMÁSIO, 2003).

2.3 Crimes virtuais impróprios

Os crimes virtuais denominados impróprios (ou mistos), são aqueles realizados no intuito de atingirem um bem jurídico comum, ou seja, que utilizam do computador apenas como *modus operandi* para a realização de atos ilícitos. Difere-se dos crimes próprios pela não essencialidade do computador para a concretização do ato ilícito, podendo se dar através de outras formas, não necessariamente pela via virtual para chegar ao fim desejado, como por exemplo em casos de pedofilia.

Assim expõe Damásio:

> [...] Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não computacionais ou diversos da informática. (DAMÁSIO, 2003).

Greco Filho (2000) adere à seguinte divisão: condutas perpetradas contra um sistema informático e condutas perpetradas contra outros bens jurídicos. Segue observação do autor.

> Focalizando-se a Internet, há dois pontos de vista a considerar: crimes ou ações que merecem incriminação praticadas 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, como, por exemplo, o homicídio. O crime, no caso, é provocador, do resultado morte, qualquer que tenha sido o meio ou a ação que o causou. (GREGO FILHO, 2000, p. 3).

Em todas as classificações existem distinções a avaliar e pontos em comum; algumas posições atribuem os meios eletrônicos como objeto protegido (bem jurídico) e meios eletrônicos como meio de se atingir outros bens. Esta classificação torna-se umas das mais pertinentes, tendo em vista que abarca mais opções acerca das práticas. (CRESPO, 2011, p.63).

2.4 Aspectos penais do sujeito ativo em crimes virtuais

A imputação objetiva ao agente e a comprovação da realização do ato ilícito é extremamente difícil, tendo em vista a dificuldade de identificação física do sujeito ativo. Dificuldade esta ligada a necessidade em se obter um perfil do infrator, de rastrear prováveis grupos organizados que praticam esta modalidade de crime.

Neste contesto, encontramos os *hackers*, pessoas que aproveitam de seu conhecimento técnico para adquirirem ou modificarem informações sigilosas por meio de dispositivos, programas ou pela rede de computadores, promovendo a prática de atos ilícitos.

Desta feita, crer-se que hacker é apenas o gênero e as espécies de *hackers* podem mudar de acordo com as suas práticas, assim, uma das espécies a ser citada são os *crackers*, palavra que foi criada no ano de 1985 por *hackers* que não concordavam com a utilização do termo *hacker* pela imprensa para definir técnicos ou usuários de computadores que cometessem ações ilegais ou que causassem transtornos para outras pessoas. (NUNES, 2015, p.20).

Em meio às ramificações do gênero, podemos ainda apresentar os denominados *lamers*, chamados de *wannabes* ou *script-kid*, que se passam como *hackers*, atuando na prática de pequenos atos ilícitos, pelo conhecimento informático limitado e por não apresentarem grande risco a sociedade. Pode-se dizer que, são apenas figuras leigas em comparação aos grandes *hackers.* E por fim temos os *phreakers*, indivíduos que praticam crimes específicos direcionados para a área da telecomunicação, e os *defacers*, famosos por invadirem páginas de sites pela internet modificando seus conteúdos. (CARNEIRO, 2012).

Classificando os perfis, podemos ter uma noção de como essas pessoas agem e o que pretendem de uma forma geral, porém o que devemos indagar é como podemos identificá-los antes que cometam tais crimes. Portanto, quando falamos em sujeito ativo, é importante que se obtenha o mais rapidamente qualquer informação, que possa servir como fonte de investigação.

2.5 Aspectos penais do sujeito passivo em crimes virtuais

Quando falamos de um crime específico logo sabemos quem é o sujeito ativo e passivo da conduta, quem realizou e em quem recaiu a ação ou omissão, no caso dos crimes virtuais de forma generalizada, a única afirmação cabível é que será sempre uma pessoa física ou jurídica ou uma entidade titular seja pública ou privada titular do bem jurídico tutelado, sempre haverá o sujeito passivo, ou seja, alguém que está sendo lesado enfim o que sofre a ação. (CARNEIRO, 2012).

Portanto, o sujeito passivo da infração penal pode ser qualquer indivíduo normal, pessoa física, ou até mesmo uma pessoa jurídica, haja vista poder, por exemplo, ter seus bens desviados, seu patrimônio deteriorado ou mesmo ter informações violadas. Ambas são capazes de determinar a ação do agente criminoso. (CARNEIRO, 2012).

Em relação às pessoas físicas, podemos afirmar que pela dificuldade de punição e pelas formas de investigação, muitas vezes deficitária, as vítimas acabam por não denunciarem os crimes praticados contra elas, dando assim aos infratores tempo para se livrarem de provas que os incriminem.

3 DOS CRIMES VIRTUAIS

Para que possamos ter uma maior compreensão deste tema, é essencial entendermos que a definição dos crimes informáticos está inteiramente entrelaçada ao conceito de criptografia.

Entende-se como criptografia, como sendo o conjunto de técnicas sofisticadas que transformam informações inteligíveis em algo que se torne incapaz à compreensão de agentes externos, ou seja, são códigos criados para desorientar e ocultar informações aos criminosos. Prática tão antiga quanto à própria humanidade, essa linguagem codificada era utilizada em mensagens secretas durante os conflitos entre Grécia e Pérsia, no período de Alexandre o Grande, e também muito utilizada pela Alemanha Nazista durante a Segunda Guerra Mundial.

Conforme a tecnologia se desenvolvia, a criptografia também se inovava, com isto despertando o interesse de grandes especialistas em estuda-la mais profundamente. Por ser uma ciência caracterizada pela técnica de ocultação, conclui-se que as primeiras noções de cibercriminalidade originaram-se da vontade de se obter ainda mais informações de caráter sigiloso, ocasionando o surgimento de grandes peritos especializados em técnicas de decifração de códigos secretos. (ROCHA, 2017).

Conhecido como o pai da computação, o britânico Alan Turing foi um renomado cientista matemático e criptoanalista que exerceu um papel fundamental durante a Segunda Grande Guerra pelo seu trabalho na área da criptografia a serviço da inteligência britânica, se tornando uma das principais figuras responsáveis pela quebra de códigos alemães durante os anos de conflito. Pode-se dizer que Turing foi o maior responsável pelo avanço da criptografia como ciência, pois expôs a fragilidade dos sistemas época buscando aprimora-los. (SCHECHTER, 2016)

Após décadas de desenvolvimento e aperfeiçoamento, nascem do conceito de criptografia as primeiras noções de internet. Na época, o único interesse ao criar este sistema, considerando-se o período histórico, era de caráter bélico e não comercial ou recreativo, pois tal expansão se deu algumas décadas após sua idealização. Assim, no auge da Guerra Fria, surgiu a ideia de criação desse sistema. (ROCHA, 2017)

Por fim, com o passar dos anos, toda a estrutura da internet foi se modificando pelas diversas inovações tecnológicas ocorridas, isso fez com que esta se tornasse o principal meio de acesso a informação em todo o mundo, abrangendo aos poucos todas as classes sociais, deixando de ser restrita apenas para alguns.

3.1 Noções gerais sobre cibercriminalidade

O termo cibercrime surgiu na cidade de Lyon (França), em uma reunião do G8 (Grupo dos Oito) realizada em 1990, em que se analisou e discutiu os crimes praticados com o auxilio de aparelhos eletrónicos utilizados como meio de disseminação de informações pela internet e as formas de combate a ameaçã que surgira. Desde então, o termo foi usado para descrever as demais formas de crimes praticados na internet e em redes de telecomuniação.

Mas, devido ao crescimento tecnológico, o combate a estes crimes tornou-se uma tarefa difícil, fazendo com que alguns indivíduos com conhecimento em informática passassem a se aprimorar e utilizar esses conhecimentos para roubar informações criptografadas, como já havia sendo feito há muito tempo, para obter proveito econômico ou ainda, por mera diversão. (JESUS e MILAGRE, 2016)

Assim, estes indivíduos ganharam a nomenclatura de *hacker*s, que significa programadores de extrema habilidade, ou seja, alguém que secretamente acessa e obtém informações do sistema informático de outra pessoa, subtraindo ou modificando-as, sem autorização para fins ilícitos.

Pela facilidade na compra de produtos pela internet e ofertas tentadoras, as vítimas muito das vezes acabam expondo suas informações pessoais em sites que foram fraudados por criminosos. Ocorre-se corriqueiramente no setor turístico no qual as pessoas compram pacotes de viagens em sites que pensam serem seguros, mas que já foram fraudados, portanto é importante que se busque a procedência destes.

Desta forma, com o desenvolvimento tecnológico e a popularização da internet, a quebra de códigos sigilosos e invasão de sistemas se tornou um negócio altamente lucrativo, com existência até mesmo de um mercado próprio para tais práticas.

A internet não só facilitou o acesso ilegal a informações e objetos de propriedade intelectual e artística, como também criou uma espécie de realidade virtual. Os usuários até desenvolveram uma linguagem, um meio de interação social, próprios dessa realidade. Nesse meio, direitos básicos do cidadão garantidos pela Constituição Federal, como a igualdade, a privacidade e a dignidade, foram sobrepujados e violados, uma vez que o braço da lei ainda não alcançava esses infratores. (ROCHA, 2017).

Alguns crimes como pedofilia, tráfico, pirataria, racismo, até mesmo terrorismo estão sendo praticados constantemente por meio da internet. Por conta disso, muitos países juntamente com o Brasil vêm buscando soluções para resolver os transtornos provocados por essa nova onda de crimes.

Muitos utilizam dessa maravilha moderna chamada internet para extrapolar seu direito e ferir o alheio, através do anonimato, acreditando jamais serem descobertos. Mas o direito brasileiro, como exemplo, vem lidando com essa questão dos crimes virtuais há muito tempo, buscando por meios legais alcançar os infratores adequando à norma no plano virtual e aplicando punições de acordo com o Código Penal Brasileiro.

Atualmente no ordenamento jurídico brasileiro, existem as seguintes leis aplicáveis aos cibercrimes. Podemos citar, a **Lei nº 12.737/2012**, apelidada de “Lei Carolina Dieckmann”, temos ainda a **Lei nº 8.069/90** (Estatuto da Criança e do Adolescente), a **Lei nº 9.609/98** (Lei do Software), a **Lei nº 7.716/89** (Lei do Crime Racial), e a **Lei nº 7.170/83** (Lei de Segurança Nacional) . A legislação brasileira também possui a **Lei nº 12.965/2014**, denominada Marco Civil da Internet, que compõe o conjunto de normas cibernéticas, o qual estabelece princípios e garantias, direitos e deveres aos usuários para o uso da internet no Brasil.

3.2 Os crimes contra a honra e o bullyng na internet

Quando praticados pela internet, o assédio moral, a calúnia, a injúria e a difamação, possuem uma extensão bem maior. É imprescindível uma punição mais severa ao agente que comete estes crimes, mesmo que não fossem tipificados, uma que vez que o dano causado tem grandes na vida das pessoas.

Deve-se lembrar que qualquer informação caluniosa e difamatória associada ao nome da pessoa ofendida, estará na internet para sempre, afetando a moral do indivíduo e sua imagem perante a sociedade. Por tanto, esses delitos que atacam a imagem e a moral, bens imateriais da pessoa humana, quando praticados através da internet, submetem o ofendido a uma humilhação contínua e perdurante.

A intimidação geralmente ocorre anonimamente, por meio de mensagens ou imagens compartilhadas das vítimas na internet que, dificilmente, serão apagadas ou terá rastreado seu ponto de compartilhamento. Existem aqueles que culpam o avanço tecnológico por tais males, porém, as novas tecnologias em grande parte são utilizadas em prol do interesse social, e possuem papel fundamental no desenvolvimento humano em diversos setores.

Para a autora Beatriz Santomauro (2010), nessa questão quando envolve jovens entre 15 e 29 anos de idade, é ainda mais preocupante, pois durante a adolescência os efeitos provocados por esse tipo de violência são mais intensos. Quando praticado em escolas, o cyberbullying, que significa assédio online, tem repercussões ainda maiores, pois dura vinte e quatro horas por dia e é capaz de alcançar o jovem onde ele estiver. Assim, cabe aos responsáveis bem como às escolas, instruir esses jovens a uma utilização consciente e produtiva da internet.
Neste seguimento, dispõe o artigo 18 do Estatuto da Criança e do Adolescente (Lei nº 8.069/90) que “é dever de todos velar pela dignidade da criança e do adolescente, pondo-os a salvo de qualquer tratamento desumano, violento, aterrorizante, vexatório ou constrangedor”.

Importante ressaltar que, esta forma de intimidação acarreta grandes problemas emocionais as vítimas, as vezes inreparáveis. Outro aspecto importante de se destacar é, a continuidade dessa prática, que antes ficava restrita aos períodos escolares, para o meio digital.

Portanto, é importante a participação dos pais e educadores no sentido de preservar a dignidade e a integridade de jovens e crianças vítimas do *bullyng*, os ensinando como interagirem socialmente de maneira mais saudável e, concientizando-os em sobre os riscos do uso indevido da internet.

3.3 O racismo virtual

O assédio e intimidação na internet está por toda parte, sem restrição de classe econômica, sendo as vezes disseminado por pessoas que fazem parte de algum grupo alvo de preconceito. Desde sempre, o racismo é considerado o maior tipo de preconceito na sociedade, provocando ainda mais indignação no âmbito da internet. (ROCHA, 2017).

Não obstante a previsão do art. 5º, inciso XLII, da Constituição Federal estabeleça que a prática do racismo constitui crime inafiançável e imprescritível, as redes sociais e fóruns de debate online se tornaram instrumento de disseminação de ideologias discriminatórias e preconceituosas, onde a maioria das pessoas não se importam por estarem cometendo o crime de racismo.

Encontramos a tipificação deste no artigo 20, parágrafo 2º da lei nº 7.716, de 5 de janeiro de 1989, que dispõe da seguinte forma:

> **Art. 20.** Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional. Pena: reclusão de um a três anos e multa. (...) § 2º Se qualquer dos crimes previstos no caput é cometido por intermédio dos meios de comunicação social ou publicação de qualquer natureza: Pena: reclusão de dois a cinco anos e multa.

A redação do artigo supra foi inserida em 1997, pela lei nº 9.459. Nessa época, a internet já havia se difundido pelo mundo como meio de entretenimento. Assim, percebe-se que ao empregar a expressão genérica “meios de comunicação social ou publicação de qualquer natureza”, o legislador abrangeu todos os meios de comunicação existentes na promulgação e durante a vigência da lei, portanto, compreendendo a internet, a televisão, os jornais, o rádio, etc. (ROCHA, 2017, p.22).

No ambiente real, este tipo de crime é praticado em todos os setores da sociedade, na grande maioria em cidades de baixo desenvolvimento humano, mas em se tratando de ambiente virtual, tais circunstâncias se tornam equivalentes, fazendo com que a propagação desta se torna quase inalcançáveis.

Portanto, identifica-se que racismo e a injúria racial são tipos penais diferentes, o primeiro está previsto na lei supracitada e tem como alvo a dignidade de toda uma comunidade de indivíduos indeterminados, em razão de sua raça. Já a injúria racial possui caráter personalíssimo, por ser dirigida a um indivíduo. (ROCHA, 2017).

3.4 Pornografia infantil

Pedofilia é um ato de perversão e forma duentia de satisfação sexual que leva um indivíduo, homem ou mulher adulto, a se sentir sexualmente atraído por crianças. A pedofilia sempre foi um asssunto muito discutido em todo mundo, mas com a popularização da internet ficou mais em evidência o real tamanho deste problema, surgindo assim, a necessidade de se estudadar e analisar no âmbito jurídico e psicológico esta prática mais profundamente. Apesar de causar repúdio por boa parte da sociedade, infelizmente, a internet se tornou um grande mercado de compartilhamento de conteúdo pornográfico infantil.

O Código Penal, em seu artigo 234, descreve:

> **Art. 234.** 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 à divulgação ou comercialização de material erótico envolvendo crianças ou adolescentes. (MARTINS, 2017, p.21).

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. (MARTINS, 2017, p.21).

O Estatuto da Criança e do Adolescente 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 Primeira Turma:

> **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. (MARTINS, 2017, p.22).

3.5 Estelionato

O estelionato é um crime muito praticado dentro do ordenamento jurídico brasileiro, em que indivíduos visão obter vantagens em proveito próprio ou para terceiro por meio de métodos enganosos, variando-se as condutas conforme os meios eletrônicos empregados. O Código Penal em seu artigo 171 trás a tipificação de tal conduta:

> **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 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 a fim de atualizar seus dados cadastrais, tendo assim, criminosas formas de adquirir informações pessoais ou confidenciais daquele usuário. (MARTINS, 2017, p.23).

São diversas as ferramentas utilizadas no combate a estes e-mails indesejados, uma destas formas seria a atualização de sistemas de proteção como *Firewall e Antivírus*, os quais servirão como barreiras para potenciais intrusos, protegendo assim, possíveis transferências de dados. (MARTINS, 2017).

3.6 Invasão de privacidade

A rede cibernética com suas facilidades trazem riscos em grande parte não vistos pelos usuários. Especialistas afirmam que é necessário ter conhecimento dos perigos e estar sempre atentos, pois a partir de um simples clique, algo que é privado pode se tornar público na internet.

O crime de invasão à privacidade deu um salto enorme nos últimos anos. A quantidade de informações, documentos, fotos, vídeos e outros tipos de arquivos obtidos pelos criminosos são imensas, esses dados dizem respeito tanto a

intimidade da pessoa física quanto informações privadas de pessoa jurídica, tais como bancos, grandes empresas e diversas outras instituições. (OLIVEIRA, 2017).

Mesmo com o avanço tecnológico no campo do Direito, indivíduos de conduta repudiável aproveitam da dificuldade que o judiciário possui de acompanhar e solucionar os litígios advindos desse avanço para praticarem seus crimes. Porém, o direito brasileiro vem se adequando a essas mudanças, a partir da solução de conflitos auxiliada por estas mesmas tecnologias.

No ano de 2012 um ato praticado contra uma figura pública serviu de estopim para a criação de uma lei que combatesse estes ilícitos. A Lei 12.737/2012 surgiu a partir do projeto de Lei nº 2.793/2011, que foi aprovado após o caso da atriz Carolina Dieckman, que teve seus dados acessados por *crackers* que, através de um e-mail infectado que atriz teria dado um click, acessaram seu computador pessoal, obtendo fotos íntimas da atriz, inclusive nua, e fotos familiares com o filho de apenas quatro anos de idade. Logo depois, ficou comprovado que, de fato, foram hackers do interior de minas Gerais e de São Paulo que praticaram o delito. A atriz foi chantageada pelos criminosos que exigiram o pagamento de R$ 10 mil reais para que as fotos não fossem divulgadas nas mídias sociais. (MELO, 2017).

Com a promulgação da referida lei, mudanças em nosso ordenamento foram realizadas, por meio das alterações dos artigos 154, 154-A e 154-B, como também os artigos 266 e 298 todos do Código Penal. Destaca-se abaixo como exemplo o artigo 154-A com a nova 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: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico. § 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: Vigência 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 obtidas. § 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.

Com a atualização deste artigo do Código Penal percebe-se que a invasão de dispositivos informáticos alheios passou a ser configurado crime, o legislador aponta que independe de o dispositivo estar ou não conectado à rede mundial de computadores, também conhecida como internet, configura o crime a simples invasão do dispositivo sem a autorização do proprietário. O praticante desta conduta antijurídica poderá ser preso ou pagar multa caso venha a cometê-la, inclusive poderá ter sua pena majorada de, caso o crime seja cometido em acordo com as hipóteses previstas no artigo, sendo as vítimas políticos, a pena poderá variar de 6 (seis) meses à 2 (dois) anos. (OLIVEIRA, 2017, p.30).

4 DA INVESTIGAÇÃO POLICIAL

Para se iniciar a investigação policial, é essencial que o agente investigatório, identifique qual forma o usuário utilizou para a prática delituosa, assim, obterá melhores resultados na investigação desses crimes ocorridos virtualmente. Por isso é de grande importância compreender como funciona a internet e as formas maliciosas que ela pode fornecer.

Cumpre ressaltar alguns aspectos básicos quanto aos procedimentos na execução dos crimes, para se entender o grau de dificuldade existente na investigação policial nos crimes virtuais. Em meados da década de 1950 quando ainda não existia a internet, para que uma organização criminosa praticasse um ato ilícito, era necessário o contato físico do criminoso com a vítima, pois desta maneira a organização promoveria o encontro de vítima e criminoso para a obtenção do “produto”, efetivando o contato em local físico, consumando o crime. (PAGNOZZI, 2018).

Então se a polícia não tomasse conhecimento do ato criminoso praticado, os membros da organização e o cliente se dispersariam na sociedade. Entretanto, se a polícia conseguisse descobrir e intervir, desmancharia parte da organização, identificaria alguns dos membros dela, seus meios de operação, algumas das práticas corriqueiras da organização, bem como os locais habituais de encontro e também o consumidor final.

Mas, se fosse aos tempos atuais, com o avanço da internet, esta mesma organização seria impossível que esta não se valesse dos recursos tecnológicos para efetivar a prática do crime. Certamente com a tecnologia, usariam a internet para comunicação interna entre os integrantes em diversos locais. O meio virtual acaba facilitando também a divulgação e compartilhamento de conteúdos ilícitos, como vídeos sexuais, uma vez que não se faria mais necessário a presença física do consumidor para a obtenção do material. Sem o local físico, a perspectiva de uma eventual apreensão dos produtos ilícitos, da identificação dos criminosos e dos consumidores, e até mesmo um possível resgate de vítimas é deteriorada.

A grande adversidade de se obter provas no mundo virtual esta ligada a dificuldade de rastreamento, ou seja, elas podem ser facilmente: ocultadas, apagadas, alteradas, editadas, excluídas ou perdidas. Isso se diferencia muito das investigações policiais no mundo real, uma vez no meio físico é muito mais difícil de

destruir por completo evidências geradas pelas ações humanas. Já, no mundo virtual, com essa possibilidade, o campo de acesso aos vestígios é muito mais amplo e dificultoso, o que demanda mais esforço de análise criminal. Além disso, devido à globalização, um infrator pode praticar esses atos de qualquer parte do mundo, pela facilidade de acesso a internet.

Quando se trata de um dano causado à vítima no mundo real, pode-se perceber que a reação contra a prática sofrida na maioria das vezes é imediata, sendo que no mundo virtual ela talvez demore muito tempo até perceber que seu computador foi infectado, ou suas informações violadas, fazendo com que muitas das evidências relacionadas ao fato criminoso se percam. Dessa forma, é comum que os *crackers* se encaminhem em maior quantidade para esta finalidade.

Nos tempos atuais, os crimes cibernéticos muitas vezes ocorrem devido à ignorância dos usuários, que praticam delitos como o cyberbullying, e também pelos obstáculos que a polícia investigativa encontra para lidar com tais delitos. Outro fator é a banalização e divulgação de informações que ensinam usuários comuns a terem acesso a documentos privados invadindo sistemas e até contas pessoais de outras pessoas. Tornou-se muito comum, inclusive, pessoas que obtiveram informações sobre como *hackear* redes sociais ou sistemas de empresas, realizarem chantagens, dizendo que irão divulgar informações pessoais e sigilosas das vítimas em troca de recompensa. (PAGNOZZI, 2018).

Em se tratando destes casos, qualquer pessoa que possua um mero conhecimento de informática é capaz de pratica-los, o que explica o enorme fluxo de denúncias nesse sentido. As redes sociais também se tornaram grandes alvos dos criminosos conforme foram se tornando mais populares, essa popularização fez com que muitas economias se fortificassem, mas consequentemente a criminalidade se introduziu a esse meio.

Pode-se dizer que a internet é abrangente, no sentido que ela alcança democraticamente todos os países do globo. Porém, não são todos os países que estão conectados à rede mundial. Em comparação com os crimes que ocorriam antes da Internet, em que a abrangência dos crimes e das organizações criminosas se limitava a possibilidade de estarem fisicamente em vários locais diferentes, os crimes virtuais abrem oportunidade para todos os países que estejam conectados na rede. Em crimes como a pedofilia existente na *deep web*, a maior dificuldade encontrada pela polícia na identificação e no combate aos compartilhamentos de

conteúdos sexuais é que os criminosos fazem as informações serem transmitidas e salvas por meio de diversos servidores. Esse fator torna a ação da polícia quase que inexistente, visto que o trabalho de identificação desses servidores demanda muito tempo e recursos financeiros. (PAGNOZZI, 2018).

Além disso, defronta-se com outro problema: o da competência territorial. O combate a esses crimes ocorre pelas autoridades capacitadas em território nacional, porém, quando estes agentes estão em outros países, os procedimentos são outros. (PAGNOZZI, 2018, p.34).

Na maioria dos casos, as grandes empresas e órgãos públicos possuem endereços de IP estáticos, enquanto que os usuários domésticos utilizam de IPs dinâmicos, ou seja, cada vez que é estabelecida uma conexão é gerado um número diferente de IP. Portanto, para se identificar quem utilizou o IP, é necessário solicitar à concessionária do serviço a quebra do sigilo da informação de quem esteve conectado em determinado dia. (PAGNOZZI, 2018, p.35).

Outra ferramenta muito útil é o reconhecimento através do domínio utilizado. Para se criar um website é necessário registrar o seu domínio na internet, sendo que este deverá estar disponível, ou seja, não poderá haver dois domínios iguais. Portanto, para identificar o dono do domínio, é preciso saber em nome de quem foi realizado o registro. Porém, a identificação do responsável se torna complexa visto que não são exigidos documentos para o registro, o que facilita fraudes. Através do site da IANA26 (Internet Assigned Numbers Authority) que no português significa Autoridade para Atribuição de Números da Internet, podem ser solicitados dados aos gestores de cada país, solicitando informações sobre o responsável pelo site. E no Brasil, através do site www.registro.br. (PAGNOZZI, 2018, p.36).

Portanto, obtendo o endereço IP e os dados do responsável pelo domínio, é possível chegar até os autores do crime. É importante que o investigador esteja atento a todo tipo de conteúdo exposto no site, uma vez que por meio deste pode-se conseguir informações como e-mail, endereço, telefone, que podem beneficiar o trabalho da polícia. (PAGNOZZI, 2018, p.36).

Além disso, deverá as autoridades competentes registrar essas informações para que não sejam perdidas por meio de impressão, *print screens* e até mesmo através do download dos conteúdos que servirão como prova, mantendo a originalidade dos documentos para que possam servir de base de localização dos criminosos, e também para que se evitem possíveis questionamentos durante o

curso do processo penal sobre a veracidade das informações utilizadas. (PAGNOZZI, 2018, p.36).

4.1 Legislação nacional aplicável

Atualmente, a legislação brasileira já abrange os principais crimes virtuais, assim, mesmo que não os exemplifique separadamente, o Código Penal Brasileiro em seus artigos trás a tipificação destas condutas, portanto, podemos analogicamente aplicá-las ao caso concreto. Ou seja, os crimes virtuais terão as mesmas penalidades aplicadas aos crimes de natureza real, como por exemplo, o crime de calúnia tipificado no artigo 138 do Código Penal.

> **Art. 138.** Caluniar alguém, imputando-lhe falsamente fato definido como crime: Pena – detenção, de 6 (seis) meses a 2 (dois) anos, e multa.
> (Redação dada pela Lei nº 2.848, de 1940).

Portanto, o agente que caluniar algum indivíduo por meio do uso da internet, responderá pelo crime com base na pena prevista no artigo 138 do Código Penal.

Entretanto, sempre foi necessária a existência de leis específicas para garantir maior efetividade e segurança jurídica por parte do judiciário no combate aos crimes cibernéticos. Assim, no ano de 2012, com a promulgação das Leis 12.735 e 12.737, a possibilidade de responsabilização do agente e daqueles que invadem dispositivos para obterem dados se tornou mais concreta. A Lei nº 12.735 veio a regulamentar a ação da polícia judiciária, em que se pode ler:

> **Art. 4º.** Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.
>
> **Art. 5º.** O inciso II do § 3º do art. 20 da Lei nº 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação: “Art. 20. II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio.

Houve muitas críticas a essa lei devido a um evidente retrocesso legislativo em comparação à Convenção de Budapeste (tratado firmado internacionalmente no âmbito do conselho Europeu para definir de forma harmônica os crimes praticados

por meio da internet e as formas de persecução). Visto que esta pretendia uma vigilância exacerbada das práticas na Internet, ficou claro que de forma alguma os cibercriminosos seriam prejudicados pela nova lei, e sim os próprios usuários que, acabando com a navegação anônima, estariam completamente expostos às corporações que rastreiam dados dos internautas, aos governos de países autoritários e os próprios criminosos que teriam ainda mais facilidade de obter informações. (PAGNOZZI, 2018).

Daí surgiu uma urgência constitucional na criação do Marco Civil da Internet. Já na Lei 12.737, durante sua criação ocorreu o incidente com a atriz Carolina Dieckmann, que teve seu dispositivo invadido e fotos íntimas de seu computador divulgadas, portanto, a lei ficou conhecida carregando seu nome. Esta lei visa tipificar os delitos informáticos tratando das invasões a dispositivos informáticos, da interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública e da falsificação de documento particular e cartão. E, além disso, tipifica condutas que não eram até então tratadas como infração penal.

Porém, houve descontentamento por parte de muitos com relação a baixas penas atribuídas a esse tipo de infração, não servindo necessariamente para coibir tais condutas. Também, tais leis não esgotaram toda a necessidade de especificar as diversas possíveis formas de delitos. (PAGNOZZI, 2018, p.42).

Observa-se:

> **Art. 2º.** O Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:
>
> "Invasão de dispositivo informático - **Art. 154-A**. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

Como podemos notar, a lei prevê que a invasão a dispositivos com o intuito de obter, adulterar ou destruir dados é infração penal punível de três meses a um ano, mas não prevê os casos de bisbilhotagem, por exemplo, em que o agente tem por intuito apenas acessar dados para proveito próprio ou para chantagear a vítima, ou nos casos em que o criminoso distribui esses arquivos roubados. Então, se o agente

não violar nenhum dispositivo de segurança, não terá cometido nenhum crime. (PAGNOZZI, 2018, p.43).

Segundo Fernando Peres, quando questionado a respeito dos problemas do legislativo na hora de criar leis:

> Eu tenho um medo muito grande no processo de criação de leis. Vejo ainda que leis que tratam de áreas específicas como a tecnologia, acabam recebendo muita influência de empresas que possuem algum tipo de interesse. E grandes provedores de internet no Brasil, possuem representantes de relações governamentais, que visam impedir que algumas leis sejam aprovadas junto ao Congresso. Agora, na hora de se criarem leis técnicas, apesar de muitas colaborações que recebem, acabam criando previsões que não são inúteis ou são impossíveis de ser realizadas. Como por exemplo, a Lei Carolina Dieckmann, que possui artigos tão específicos, que muitos crimes podem não ser enquadrar. [...] Quando se trata de questão criminal, temos que ser pontuais, não podem fazer analogias e interpretações em desfavor do réu. (PERES, 2017).

Em 2014, foi sancionada a Lei 12.965, também conhecida como Marco Civil da Internet que visa regulamentar o uso da Internet por meio de princípios, garantias, direito e deveres para os usuários. A ideia do projeto surgiu com a resistência à Lei de Azeredo (12.735/12), como uma proposta do Poder Executiva a Câmara dos Deputados e aprovada em 23 de abril de 2014. Ela serve para regular a utilização, garantir a privacidade, a inviolabilidade da vida privada, bem como para garantir que a Internet cumpra a função social devida. É regida a partir de princípios como os da neutralidade, da reserva jurisdicional, da responsabilidade dos provedores, dentre outros. Foi de extrema importância para impor principalmente obrigações de responsabilidade civil aos usuários e provedores. (PAGNOZZI, 2018, p.43-44).

4.2 Medidas de proteção contra os cibercrimes

Por mais que pareça difícil se proteger dos ataques dos criminosos, tendo em vista a quantidade de crimes que são realizados, existem formas para impedir tais práticas, como a utilização de programas de antivirus e senhas em dispositivos como computadores, smartphones e tablets,visando a proteção de dados bancários, fotos pessoais, e arquivos.

Jamais realizar compras em sites sem recomendação ou que não sejam confiáveis, pois muitos criminosos se aproveitam da desatenção das vítimas para

obterem informações que lhe sejam uteis. Ter uma boa segurança para e-mails também é fundamental, e o uso das redes sociais deve ser feito com moderação, pois muitos assuntos privados caem em mãos erradas ou se tornam objeto de investigação pelo fato das vítimas não tomarem as devidas providências.

É importante se desconectar de aplicativos ou outros meios de serviço de e-mail baseado na internet, isso impede que qualquer pessoa que tenha acesso a diapositivos que foram emprestados, furtados ou roubados, tenha acesso ao conteúdo.

A SaferNet Brasil é uma entidade que não possui fins lucrativos e também possui uma cooperação com o Ministério Público Federal além de apoiar o Comitê Gestor da Internet no Brasil e a Justiça Federal, em um período de 11 anos, esta recebeu e também processou 3.861.707 denúncias anônimas, a vítima de crimes virtuais pode realizar uma denúncia anonimamente juntamente à SaferNet, antes da denúncia ser feita basta realizar a escolha da categoria do crime, inserir o site em questão ou adicionar comentários sobre a denúncia. A SaferNet poderá solicitar a retirada do conteúdo do ar para o provedor caso a denúncia proceda. (OLIVEIRA, 2017, p.40).

Destacam-se também as delegacias de repressão especializadas em crimes virtuais como outro meio de se denunciar estes crimes. São apelidadas de Delegacias Cibercrimes, presentes em vários estados no país, e caso não haja este tipo de serviço na cidade da vítima, as demais delegacias são aptas para efetuar o registro de ocorrência.

5 CONCLUSÃO

Ao fim da pesquisa pode-se compreender a relevância do tema visto que a evolução tecnológica tem se expandido mais e mais a cada dia, surgindo diversos tipos de delitos cibernéticos. Tais crimes exigem atenção uma vez que a internet tornou-se parte essencial da vida em sociedade, necessitando de normas que regulamentem as ações humanas no ambiente virtual.

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.

Abordam-se os principais delitos informáticos que assombram este ambiente, como são conceituados na visão de vários autores e principalmente a forma com que o Direito Penal busca reprimir estes crimes, uma problemática que deve ser abordada, pois da mesma forma que na vida real os crimes virtuais também devem ser passíveis de punição, para que a justiça, os bons costumes e a democracia prevaleçam.

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.

Como nenhum direito é absoluto, portanto sua extensão é limitada, cabe ao Estado, na sua forma judicial, corrigir os excessos em seu exercício, haja vista que cada direito acaba onde outro começa. Desta forma, a restrição é a única ferramenta capaz de amparar um direito violado pelo cometimento de excessos e abusos no exercício de outro direito.

REFERÊNCIAS

BRASIL. **Constituição da República Federativa Do Brasil de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm> Acesso em: 15 dez. 2019.

_____. **Código Penal (CP):** Decreto-Lei n° 2.848, de 7 de dezembro de 1940. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 19 dez. 2019.

_____. **Lei nº 7.716, de 5 de janeiro de 1989.** Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l7716.htm>. Acesso em: 02 dez. 2019.

_____. **Lei nº 8.069, de 13 de julho de 1990.** Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em: 15 dez. 2019.

_____. **Lei nº 12.735, de 30 de novembro de 2012.** Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acesso em: 03 dez. 2019.

_____. **Lei nº 12.737, de 30 de novembro de 2012.** Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 19 dez. 2019.

ANDREUCCI, Ricardo Antonio. **Legislação penal especial**. 12ª ed. São Paulo: Saraiva, 2017.

BLUM, Renato M. S. Opice; ABRUSIO, Juliana Canha. **Os hackers e os tribunais.** IBDI – Instituto Brasileiro de Direito da Informática, 9 mar. 2004. Disponível em: <http://www.ibdi.org.br/index.php?secao=&id_noticia=287&acao=lendo >. Acesso em: 25 nov. 2019.

CARNEIRO, Adeneele. Âmbito jurídico. **Crimes virtuais:** elementos para uma reflexão sobre o problema na tipificação. Artigo. Disponível em: <http://www.ambitojuridico.com.br/site/index.php/?n_link=revista_artigos_leitura&artigo_id=11529&revista_caderno=17>. Acesso em: 27 nov. 2019.

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

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

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet.** 5 ed. São Paulo, Saraiva, 2010.

D'URSO, Luiz Augusto Filizzola. **Cibercrime:** perigo na internet. Publicado em 2017. Disponível em <http://politica.estadao.com.br/blogs/faustomacedo/cibercrime-perigo-na-internet/>. Acesso em: 28 nov. 2019.

FELIZARDO, Aloma Ribeiro – **Cyberbullying Difamação na Velocidade da Luz**. 1º Ed. São Paulo. Willem Books 2010.

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

G1. **Operação de 9 países contra pedofilia na internet termina com 13 detidos.** Disponível em: <http://g1.globo.com/mundo/noticia/2016/05/operacao-de-9-paises 50 contra-pedofilia-na-internet-termina-com-13-detidos.html>. Acesso em: 04 nov. 2019.

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.

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

JESUS, Damásio de. MILAGRE, José Antonio. **Manual de Crimes de Informáticos.** São Paulo: Saraiva, 2016.

KELSEN, Hans. **Teoria pura do direito.** Tradução de João Baptista Machado. 7. ed. São Paulo: Martins Fontes, 2006.

OLIVEIRA, Felipe Cardoso Moreira de. **Criminalidade informática. 2002**. Dissertação (Mestrado em Ciências Criminais), Faculdade de Direito, PUCRS, Porto Alegre, 2002.

PAESANI, Liliana Minardi. **Direito e Internet:** liberdade de informação, privacidade e responsabilidade civil. 1ª ed. São Paulo, Atlas: 2000.
PERES, Fernando. **Entrevista concedida a Isadora Marina C. de Almeida Pagnozzi.** Curitiba, 1 de novembro de 2017.

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

SCHECHTER, Luis Menasche. **A Vida e o Legado de Alan Turing para a Ciência.** Publicado pelo Departamento de Ciâencia da Computação/UFRJ, 2016. Disponível em <http://www.dcc.ufrj.br/~luisms/turing/Seminarios.pdf>. Acesso em: 03 dez. 2019.

SILVA, Fernanda Tatiane da. PAPANI, Fabiana Garcia. **Um pouco da história da criptografia.** Publicado em Anais da XXII Semana Acadêmica de Matemática da Unioeste, 2016. Disponível em: <http://projetos.unioeste.br/cursos/cascavel/matematica/xxiisam/artigos/16.pdf>. Acesso em: 06 dez. 2019.

SANTOMAURO, Beatriz. **Cyberbulling:** a violência virtual. Publicado em 2010. Disponível em <https://novaescola.org.br/conteudo/1530/cyberbullying-aviolencia-virtual>. Acesso em: 04 dez. 2019.

PAGNOZZI, Isadora. **CRIMES VIRTUAIS: UMA ABORDAGEM JURÍDICA ACERCA DAS LIMITAÇÕES NO COMBATE AOS CRIMES CIBERNÉTICOS** . Publicado em 2018. Disponível em <https://www.unicuritiba.edu.br/images/tcc/2018/dir/ISADORA-MARINA-CASTELAN-DE-ALMEIDA-PAGNOZZI.pdf. Acesso em: 31 dez. 2019.

TATEOKI, Victor Augusto. **Classificação dos Crimes Digitais**. Publicado em 2016. Disponível em <https://www.jusbrasil.com.br/artigos/307254758/classificacao-dos-crimes-digitais>. Acesso em 11 de fev. 2020.

SCHMIDT, Guilherme. **Crimes Cibernéticos**. Publicado em 2015. Disponível em <https://www.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos>. Acesso em 15 de jan. 2020.

SILVEIRA, SOUSA,MELO, Neil, Mirian, Antônia. **Crimes cibernéticos e invasão de privacidade à luz da lei Carolina Dieckmann.** Publicado em 2017. Disponível em <https://www.jusbrasil.com.br/artigos/61325/crimes-ciberneticos-e-invasao-de-privacidade-a-luz-da-lei-carolina-dieckmann. Acesso em 22 de jan. 2020.