FACULDADE DE DIREITO DE IPATINGA

Larissa Dorneles Barbosa

CRIMES VIRTUAIS E A LEGISLAÇÃO PENAL BRASILEIRA

IPATINGA/MG

2020

Larissa Dorneles Barbosa

CRIMES VIRTUAIS E A LEGISLAÇÃO PENAL BRASILEIRA

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Faculdade de Direito de Ipatinga, como requisito parcial para obtenção do título de Bacharel em Direito.

Orientador: Prof. Renato Lopes Costa

FACULDADE DE DIREITO DE IPATINGA

IPATINGA/MG

2020

Dedico este trabalho a todos que estiveram ao meu lado, me apoiando e ajudando, por nunca me deixarem desistir e acreditar sempre na minha capacidade.

AGRADECIMENTOS

Primeiramente quero agradecer a Deus, por sempre estar ao meu lado, me protegendo e abençoando, por me acalmar e me manter firme para chegar até aqui.

Em segundo lugar, quero agradecer aos meus pais, por sempre acreditarem em mim, por nunca deixar de sonhar o mesmo sonho que o meu e estar ao meu lado nos momentos que mais precisei, por escutar meus desabafos e reclamações diárias, e por terem os mais sábios conselhos para que eu aguentasse firme essa caminhada. Ao meu irmão, que por mais estressante, sempre me protegeu. Eu amo vocês!

As minhas amigas de faculdade e de vida Bianca, Marina e Élida, por sempre estarem comigo, e principalmente nessa reta final que não foi nada fácil, sem o apoio e ajuda de vocês nada seria possível. Ao grupo Endireitando, que a todo momento se fez presente, ajudando e dando risada de tudo isso.

Agradeço também a todos os meus amigos de vida e aos amigos Unimed pela amizade e paciência, vocês foram essenciais.

Por fim, agradeço a todos que contribuíram para realização desse trabalho, sem vocês eu não teria chegado até aqui. Gratidão!

RESUMO

Esta pesquisa teve por objetivo analisar o surgimento e a evolução da tecnologia e até que ponto ela afeta a vida em sociedade. Colocando em tese principal que ela atende a maior parte dos crimes, os quais são praticados através da internet. Serão analisados também os aspectos de como ocorrem esses crimes, bem como a classificação de cada um deles e o perfil de cada criminoso. Com a evolução tecnológica surge a necessidade de adaptação do direito para a nova era tecnológica, tanto no âmbito penal quanto civil. A presente monografia, sobre o tema crimes virtuais, busca esclarecer a nova realidade digital da sociedade, mostrando os crimes e quem são os autores, como também a legislação nacional e internacional é aplicada, para que possamos compreender como são os comportamentos dos outros países diante desse crime, como também a busca pelo amparo social através das legislações vigente, verificando o que já existe e qual a importância do ordenamento jurídico coerente com a realidade para a eficaz aplicação das normas.

Palavras-chave: Crimes virtuais. Direito Penal. Avanço Tecnológico. Internet. Legislação.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

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

CETIC.BR - Centro Regional de Estudos para o Desenvolvimento da Sociedade de Informação

CC - Código Civil

CP - Código Penal

CPP - Código de Processo Penal

ECA - Estatuto da Criança e do Adolescente

PL - Projeto de Lei

PLC - Projeto de Lei Complementar

SAFERNET - Safer Internet Center do Brasil

STJ - Superior Tribunal de Justiça

WEB - Conjunto de páginas na internet

SUMÁRIO

1. INTRODUÇÃO

É nítido ver que na historia da humanidade, o avanço da tecnologia e sua modernidade, se tornou um meio necessário e totalmente indispensável para todos em seu cotidiano. Contudo, a forma fácil em que todas as informações são acessadas e usadas pela Internet, tem se tornando um grande problema para que os usuários consiga controlar e supervisionar suas atividades, pois há varias formas de se utilizar em forma anónima.

Com o surgimento desses atos ilícitos, se torna necessária a mediação do Direito Penal junto a evolução tecnológica, com o intuito de assegurar a aplicação das normas penais, de forma justa e valida. E é a partir disso que o tema e respectivo estudo se torna essencial, de uma forma em que se pode ver a condição em que se encontra a legislação brasileira para resolver esse ato ilícito.

Desta forma, se torna relevante o estudo para que possamos ver como é realizada a investigação dos crimes, no qual se encontra no anonimato o ato do agente e também como se dá os julgamentos e instruções nesses casos.

Para uma fácil compreensão do tema, é necessário entender o que são os crimes virtuais e todas suas características, também para que se possa ver o meio mais adequado para as investigações a serem feitas.

O presente trabalho visa expor o que são estes crimes e como a sociedade moderna é uma vítima potencial quando está utilizando a internet.

O segundo capítulo do presente trabalho discorre sobre o surgimento e a evolução da tecnologia na sociedade e os primeiros atos ilícitos digitais que foram necessário uma legislação especifica.

O terceiro capítulo considerará a classificação, bem como os principais tipos de crimes virtuais e como ocorrem na web, demonstrando se existe ou não tipificação legal para eles.

O quarto capitulo abordará sobre as dificuldades existentes para que seja encontrada a identificação do agente e para apurar o crime cuja obtenção de provas que comprovem a autoria.

Por fim, o quinto e sexto capítulo será analisado as leis nacionais e internacionais aplicáveis aos crimes e qual o resultado de punir ou inibir a prática ilícita por meio digital.

2. A INTERNET E O DIREITO

Para que o Direito atenda as necessidades e as normas que regulam as condutas diante da evolução do ser humano, deverá ele também acompanhar tal evolução.

Conforme o surgimento e evolução da internet, a sociedade vem caminhando rapidamente para uma geração que ira depender da informática, substituindo então vários atos da vida social pelos sistemas de tecnologia de informação. A Internet executa com rapidez cada função, tornando então o ser humano mais dependente e mais convencido para utilização das ferramentas virtuais, de uma forma que hoje, a pessoa que não aderir desse meio tecnológica se torna de tal forma "isolada" da sociedade. A respeito disso, Maciel Colliposiciona-se:

> O uso da internet possibilitou a superação da dificuldade ocasionada pela distância territorial e pela limitação comunicativa entre as pessoas em locais distantes. A voz e o papel foram desbancados do ranking instrumental de intercâmbio de mensagens. O texto exibido nas telas de computadores, produtos de linguagem binária interpretada e transmutada pelas plataformas dos computadores, elimina a distância e o tempo.[1]

Para entender essa evolução, é válido especular de onde surgiu a internet. A palavra significa "rede internacional" - advindo da união dos termos em inglês Inter (internacional) e net (rede) - e surgiu no fim do século XX. Inicialmente, despontou como ferramenta para internalizar as comunicações em casos de guerra e para estudar as relações entre ser humano e máquinas. Porém, o uso dos computadores era limitado a poucos usuários, pois basicamente era utilizado para uso militar e científico. Foi na década de 1990 que a internet tornou-se ferramenta pública e colocada como um uso necessário e fundamental para sociedade.

Coincidente com a tecnologia evoluindo, e conforme à sociedade substituiu suas ações físicas pelas ações virtuais, veio os problemas criados pela criminalidade virtual. E conforme diz Gustavo Têsta Correa, "A internet é um paraíso de informações, e, pelo fato de essas serem riqueza, inevitavelmente atraem o crime.

Onde há riqueza, há crime."A internet esta sendo um mecanismo considerado sempre como recente e que acabou modificando radicalmente toda a vida do ser humano.

Em 1980 deu inicio aos diferentes tipos de crimes virtuais, como pirataria, transmissão de vírus, pedofilia, invasão de sistemas, entre outros. Como essas práticas foram se tornando expressivas, veio a necessidade de precaução com a segurança virtual e como resultado, a intervenção do Estado para regimentar tais condutas.

O fato dos criminosos cometerem os crimes na internet, é a confiança de que lá eles estão protegidos, e isso acontece porque na sociedade ainda não existe algo que possa prevenir de possíveis atos ilícitos pelos criminosos. Pode ser talvez, pelo motivo de tal problema ser ainda relativamente novo, onde a sociedade não consiga imaginar que protegendo os computadores e dispositivos, possivelmente as condutas ilegais serão extintas.

A questão dos crimes virtuais, começou a ser preocupada pelo Brasil recentemente. Em 1988 na promulgação da Constituição foi estabelecido que tais questões de informática deveriam ser de competência do Estado. Damásio de Jesus complementa:

> O marco Civil da Internet é considerado a “Constituição da Internet”, garantindo direitos e deveres a todos os autores da Internet brasileira [...]. Fruto de um projeto nascido em 29 de outubro de 2009, [...] o Marco Civil foi uma construção colaborativa, disponível para consulta pública entre novembro de 2009 e junho de 2010,tendo recebido mais de duas mil contribuições.

O projeto de lei, após passar pela participação popular, ingressou no Congresso Nacional por iniciativa do Poder Executivo e foi sancionada pela Presidenta Dilma Rousseff em 2014, como Lei 2.216. Além disso, em 2012, com a promulgação das Leis 12.735 e 12.737, as chamadas Leis de Crimes Informáticos, o legislativo tentou tipificar as condutas ilícitas cometidas no meio virtual.

É de grande importância entender e compreender de que forma veio a acontecer os crimes virtuais. Uma vez que a Internet acabou de tornando alvo do interesse público, é de se esperar que nela também desenvolva condutas criminosas,

de uma forma que o ser humano vem a criar meios ilegais para todas as atividades de seu cotidiano. Dessa forma, deparamos com o sujeito que pratica tais condutas, que é conhecido como “ciber criminoso”, conceito que será abrangido mais adiante.

3. CRIMES VIRTUAIS

Atualmente na sociedade, tem-se a ideia de que na internet pode ser feito de tudo porque não haverá nenhum tipo de punição para os atos, porém ao pensar dessa forma é onde erramos, pois dos crimes cometidos no meio virtual, grande maioria é passível de punição. Independentemente de qual forma é realizada a pratica do crime.

Hoje, a legislação penal em vigor, possui meios para que se possa combater a maioria dos crimes digitais. Em conformidade com os pensamentos de MASSON (2016) “ao contrário das vozes lançadas pela opinião popular, a internet nunca foi um território livre, sem lei e sem punição”.

Assim como as práticas de crimes comuns se aperfeiçoam com o tempo, os crimes virtuais também tomam novas formas através do avanço tecnológico que permite e facilita suas práticas. Com o grande número de usuários na internet - que ultrapassa 3 bilhões -, é cada vez mais difícil identificar os agentes que cometem crimes na internet, se tornando assim muito delicado legislar sobre o direito eletrónico, pois sabe-se que nos crimes digitais as testemunhas são as próprias maquinas, a quais não sabem identificar o crime praticado com culpa por um praticado por dolo. O que se pode levar a punição indevida do agente.

A Safernet Brasil registrou o recebimento e processamento de 4.059.137 denúncias anônimas, ocorridas no período de 13 anos, o que demonstra o alto índice de crimes virtuais.

Pode-se dizer que os ataques realizados na internet pelos criminosos, são utilizados de vários métodos distintos para a pratica de seus crimes, visando alvos diferentes e por inúmeros objetivos. Portanto, os crimes virtuais são todos aqueles que ocorrem através ou com o auxílio de meios virtuais, sendo utilizados para a prática de atos ilegais, servindo para renovar e potencializar a execução de delitos já existentes ou para criar novos crimes.

3.1 Crimes virtuais típicos da era da tecnologia da informação

Vamos abordar, de forma clara, nos próximos subtópicos, os tipos de crimes digitais que mais são recorrentes no meio virtual, a sanção que será definida pela legislação penal e suas peculiaridades, uma vez que a maioria desses crimes não estão previstos no Código Penal, mudando apenas o ambiente onde é realizado o crime.

15 É definida pelo CERT como uma condição que, quando explorada por um cibercriminoso, pode resultar em uma violação de segurança.

16 Varredura em redes ou scan, conforme o CERT, é uma técnica que consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles.

17 Falsificação de e-mail, ou e-mail spoofing, é uma técnica que consiste em alterar campos do cabeçalho de um e-mail, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra. Definição do CERT.

18 Um ataque de força bruta, ou brute force, consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar sites, computadores e serviços em nome e com os mesmos privilégios deste usuário. Conforme definição do CERT.

19 Conforme definição do CERT, um ataque de força bruta, ou brute force, consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar sites, computadores e serviços em nome e com os mesmos privilégios deste usuário.

20 Desfiguração de página, defacement ou pichação, conforme definição do CERT, é uma técnica que consiste em alterar o conteúdo da página Web de um site.

21 Negação de serviço, ou DoS (Denial of Service), é uma técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada à Internet. Conforme definição do CERT.

3.1.1 Cyberbullying

O Cyberbulling vem da palavra bullying, cujo termo é utilizado para descrever as praticas de atos de violência física ou psicológica que ocorrem intencional e repetida, praticada pelo meio virtual por um indivíduo ou grupo de indivíduos, através de computadores, celulares e tablets, causando então angústia e dor.

De acordo com Cassanti, cyberbullying é definido como:

> A ação intencional de alguém fazer uso das tecnologias de informação e comunicação para hostilizar, denegrir, diminuir a honra ou reprimir consecutivamente uma pessoa. Contrário do tradicional e não menos preocupante bullying, que é presencial, ou seja, as ações do agressor têm lugar certo, no cyberbullying o agressor não consegue presenciar de formaimediata os resultados da sua ação, minimizando um possível arrependimento ou remorso.

Para SILVA (2010) cyberbullying trata-se da migração para o meio virtual de atitudes de violência psicológica, com o cunho intencional e repetitivo, praticado por um ou mais agressores contra uma ou mais vítimas que se encontram impossibilitadas de se defender.

Nesse meio de crimes virtuais, os tipos mais recorrentes se dão por meio de Facebook, cuja ofensa se da pela humilhação, envio de fotos adulteradas, humilhação e postagens nas redes sócias com mensagens que vem a abalar o psicológico da vitima. O delituoso geralmente está acobertado sempre pelo anonimato, permitindo assim condutas na qual não seriam praticadas por eles pessoalmente, e tal crime pode vim a evoluir e ocorrer ameaças contra a vida,disseminação de ódio racial e entre outros. Tais atitudes, podem trazer a vítima casos extremos, levando ela a um suicídio ou depressão profunda.

Nesse crimes, as principais vitimas estão entre adolescentes e crianças, e geralmente correm em ambiente escolar, mas também pode ser praticado fora dele. Geralmente esses adolescentes e crianças, criam um perfil fake em rede social para que assim pratiquem o crime, onde lá postam mensagens humilhantes e de intimidação à vitima.

3.1.2 Crimes contra a honra

O crime contra a honra, que é caracterizado com a calunia, difamação e em denegrir a imagem das pessoas, ocorrem pelo anonimato, visando assim ofender a honra objetiva e/ou subjetiva da vítima. Tais crimes contra a honra estão previsto no capítulo V, Parte Especial do CódigoPenal.

A injúria racial ou qualificada difere-se do crime de difamação, enquanto uma fere a honra objetiva outra atinge a honra subjetiva da vítima. De acordo com o Ministro Marco Aurélio apud MASSON (2016) “a difamação pressupõe atribuir a outrem fato determinado ofensivo à reputação. Na injúria, tem-se veiculação capaz de, sem especificidade maior, implicar ofensa à dignidade ou ao decoro.”

São inúmeras as ocorrências delituosas contra a honra na internet. Um exemplo desse ilícito de injúria racial, foi o caso ocorrido com a atriz Thais Araújo, que aconteceu em setembro de 2015. A atriz publicou uma própria foto no Facebook e as pessoas escreveram vários comentários maldosos que criticavam o cabelo da atriz nas redes sociais. Veja:

Imagem 1: Comentários racista contra Thais Araújo.

Fonte: <extra.globo.com>

Outro exemplo recorrente do mesmo crime, foi os ataques de haters na internet contra Titi, filha de Bruno Gagliasso e Gio Ewbank. Um deles ocorreu em 10 de novembro de 2016, onde pessoas fizeram comentários em uma foto que ambos postaram com a filha dizendo que a garota não combina com os pais e que eles deveriam devolvê-la para África, pois o lugar dela seria lá. Além de dizer que deveriam adotar uma criança que “parece” com eles, dos olhos claro e loiro. Observe:

Imagem 2: Injúria racial contra filha de Giovanna Ewbak

Fonte: <observatoriodatelevisao.bol.uol.com.br>

Está previsto no art. 140, §1º do Código Penal, a injúria qualificada, com pena de reclusão, de um a três anos, sem qualquer prejuízo de multa.

Vejamos também que a Lei 9.459/97 modificou o art. 140 do Código Penal, acrescentando-lhe o § 3o, que prevê a injúria qualificada pelos elementos de raça, cor, etnia, religião e origem, dando-lhe a mesma pena do crime do artigo 20, caput, da lei especial 7.716/89.

Para que ocorra a injúria racial é necessário, além do quesito pessoal, a designação de qualidade negativa à vítima que consiste em ofende-lá com elementos que atribua a sua raça, cor, etnia, cultura, religião ou origem. Esse tipo de ilícito reclama que a ofensa seja dirigida à pessoa ou pessoas determinadas, diferente do racismo, que atinge um grupo ou pessoas indeterminadas, discriminando toda a integralidade de uma raça.

Cumpre lembrar, que o delito é afiançável e prescritível, além se estar previsto no código penal, diferente do racismo que se encontra na legislação especial, qual seja, Lei 7.716/1989.

A difamação, delito este que esta previsto no artigo 139 do Código Penal, é constituído quando o indivíduo ofende a honra objetiva da vítima imputando-lhe fato ofensivo à sua reputação.

Lembrando que, não é necessário que essa imputação seja verdadeira, desde que seu objetivo seja o de ofender a vítima. O legislador, buscando esclarecer esse tema, ao tipificar o crime de difamação, deixou nítido que as pessoas não podem fazer comentários maldosos sobre a vida alheia, pois não lhe diz respeito.

3.1.3 Racismo

O Racismo consiste em um crime, cujo preconceito é baseado na discriminação, manifestações de ódio, aversão, coação, agressão, intimidação, difamação ou exposição de pessoa ou grupo. A discriminação se da a um ato de fazer distinção, sendo o racismo um caso particular da discriminação, onde qualquer pensamento ou atitude de separação por raça é classificado como racismo.

Hoje em dia, onde se impera uma grande diversidade de pessoas e raças, não deveria ser “normal” a ocorrência de racismo, e ele esta previsto no topodos crimes que mais ocorrem atualmente. Tanto no âmbito da fama quanto com os anónimos.

Como já dito anteriormente, as pessoas imaginam tudo pode ser dito ou feito nas redes sociais, e que ao pratica-los não terão consequência alguma de seus atos. A internet acaba criando uma sensação ao individuo de impunidade, com um pensamento equivocado a respeito, onde ao agir assim todos seus atos trarão consequências, seja na esfera civil ou penal.

Um exemplo que podemos ver é o da estudante de uma estudante de direito do estado de São Paulo, Mayara Petruso, que usou sua conta no Twitter e Facebook, após a derrota do candidato às eleições presidenciais, José Serra, no ano de 2010, para fazer comentários ofensivos aos nordestinos, dizendo que não são pessoas e que deveriam ser mortos por meio de afogamento. Veja:

Imagem 3: Tuites com conteúdo racista de Mayara

Fonte: <idgnow.com.br>

Segundo o doutrinador Masson (2016), racismo “é a divisão dos seres humanos em raças, superiores ou inferiores, resultante de um processo de conteúdo meramente político-social.” Dessa divisão gera a atitude desumana de discriminação e preconceito entre os indivíduos do mesmo país, estado ou cidade.

A CFRB/88 não faz qualquer distinção entre os seres humanos, pois todos são iguais. Garantindo aos brasileiros ou estrangeiros o direito à vida, liberdade, igualdade, segurança entre outros direitos previstos no Título II do diploma legal acima referido.

A prática do racismo constitui como crime inafiançável e imprescritível, sujeito à pena de reclusão, disposto expressamente no artigo 5º, XLII, da Constituição Federal/88. Tendo em vista que todos os seres humanos são iguais, perante a lei e perante a ciência.

Nos dizeres de MASSON (2016) “não há diferença biológica entre os seres humanos, quer na essência, biológica ou constitucional (art. 5.º, caput), são todosiguais.”.

Os crimes de racismos estão previstos em Lei especial, n° 7.716/1989, que tipificou o racismo como crime e não mais como contravenção penal, penalizando assim apenas aquelas condutas preconceituosas por raça ou cor. Mas em 1997, com a Lei 9.459, foi acrescentado ao texto hipóteses de discriminação ou preconceito por etnia, religião ou procedência nacional, aumentando a pena para 1 a 3 anos. Atualmente são várias as situações que podem ser elencadas, tais como pronunciamentos preconceituosos generalizados, alcançando uma coletividade ou por segregação racial.

O artigo 20 da Lei 7.716/89 foi alterado algum temo depois, pela Lei 12.228/10, que incluiu no § 3º a possibilidade de interdição das respectivas mensagens ou páginas de informação na rede mundial de computadores. Passando a vigorar da seguinte forma:

> Art. 20. Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional.(...)
> § 2º Se qualquer dos crimes previstos no caput é cometido por intermédio dos meios de comunicação social ou publicação de qualquer natureza:
> § 3º No caso do parágrafo anterior, o juiz poderá determinar, ouvido o Ministério Público ou a pedido deste, ainda antes do inquérito policial, sob pena de desobediência:
> I - o recolhimento imediato ou a busca e apreensão dos exemplares do material respectivo;
> II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio;
> III - a interdição das respectivas mensagens ou páginas de informação na rede mundial de computadores.

Observa-se que o referido artigo é, atualmente, o dispositivo principal para tipificação dos crimes de racismos pelo meio digital. Deixando claro que qualquer crime dessa natureza, se praticado por intermédio dos meios de comunicações sociais, incluindo a internet, ou de publicação de qualquer natureza sofrerá as sanções dos parágrafos do artigo 20 da Lei que criminaliza o racismo.

3.1.4 Pedofilia e pornografia infantil

Com a popularização da Internet, deixou ainda mais evidente a pedofilia, pois é impossível não associa-la com a internet, uma vez que existe semelhança nas novas possibilidades de obter prazer e saciar desejos através das redes sociais, ocorrendo então maior expansão da prática da pedofilia, pela facilidade de transmissão de informações.

Apesar desse ato ser de grande repúdio pela sociedade, infelizmente, há na internet diversas figuras com este tipo de material.

O código penal, em seu artigo 234, dispõe:

> 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.

É de suma importância dizer que, na pornografia infantil, não é necessário que se tenha relacionamento, basta somente a divulgação ou comercialização do material envolvendo crianças ou adolescentes, diferente da pedofilia que existe uma impudência sexual, uma relação do adulto com crianças ou adolescente.

De acordo com dados divulgados da Jornada Estadual contra Violência e a Exploração Sexual de Crianças e Adolescentes, constatou que só no Rio Grande do Sul havia uma média, no início de 2013, de 10 casos por dia de menores que sofriam abuso ou exploração sexual.

De acordo com os dados divulgados pela empresa Safernet, que em 13 anos, a Central de Denúncias de Crimes Cibernéticos recebeu e processou 1.518.617 de denúncias anônimas de pornografia infantil envolvendo 312.037 URLs distintas, das quais 119.623 foram removidas, conectados à internet através de 42.188 números de IPs distintos em todo o mundo.

Somente no Brasil, no ano de 2016, foram reportados mais de 280 casos de pornografia infantil. A pedofilia no Brasil hoje, é um fator de grande preocupação e bem mais grave do que imaginamos, e ainda que se tem esforços para combater tais crimes, ainda é muito difícil de conte-los.

O Estatuto da Criança e do Adolescente, lei 8.069/90, 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.

Após o reconhecimento em Repercussão Geral pelo STF no RE 628624, a conduta de divulgar imagens, vídeos pornográficos de criança na internet atrairá a competência da justiça federal, passando a entender assim o STF que basta a divulgação e o crime já está consumado independente do meio utilizado

3.1.5 Invasão

A Invasão se da a um tipo de ataque bem-sucedido, que tem como finalidade o acesso, a alteração, manipulação ou destruição de informação de um dispositivo informático.

Essa conduta de invasão em dispositivo informático não era considerada pelo Código Penal, no entanto após a atriz Carolina Dieckman ter seu computador invadido e 36 fotos íntimas subtraídas de seu computador por cinco homens, posteriormente identificados e responsabilizados pelos crimes de extorsão, difamação e furto, e não tipificados e penalizados pela invasão do computador.

Diante do caso ocorrido contra uma figura pública, por falta de legislação que cuidasse do crime em especifico, que o congresso nacional, estimulados pela mídia, aprovaram em 2012 a Lei 12.737.

O crime de invasão informática se consuma a partir do momento em que o agente criminoso invade o dispositivo informático alheio, mediante violação indevida de mecanismo de segurança, com o propósito de obter, adulterar ou destruir dados ou informações sem autorização, instalar vulnerabilidades ou obter vantagem ilícita, não importando se este objetivo vem a ser efetivamente alcançado.

Aquele que contribuir para que um terceiro venha a utilizar dispositivo informático alheio, incorrerá na mesma pena do caput do artigo 154-A.

3.1.6 Inutilização de equipamento informático

Este tópico se trata do crime de dano, realizado por meio da rede de computadores, que se dá através da inutilização do computador ou de outro dispositivo eletrônico ou pela destruição de informações ou ou dados no sistema de informação.

Não existe previsão legal para o delito de dado informático, porém os tribunais aplicam o artigo 163, do Código Penal para tratar desse crime, tendo em vista que é o mesmo crime, porém foi aperfeiçoado a técnica para sua aplicação, que se dá através do ambiente virtual. Dispõe o artigo:

> Art.163: Destruir, inutilizar ou deteriorar coisa alheia:Pena – detenção, de um a seis meses, ou multa.

No entendimento de MASSON (2016) o dano deve ser o seu próprio fim, tendo em vista que ele não é resumido em inutilizar, destruir ou atém mesmo deteriorar coisa de outrem. Esse tipo de crime pode ser aplicado através da disseminação de vírus, boots worms, trojans, rootkits, adwares, ransomwares, entre outros.

O worms, sua principal função é deletar dados de um computador, uma vez que não necessita de um hospedeiro para se alastrar.

Os boots, tem o poder de destruição extremamente alto, onde pode-se impedir a vitima de utilizar seu aparelho, infectam o disco rígido de um dispositivo informático.

Os rootkits infectam as tarefas e processos de memória, e conseguem anular o pedido do programa que esta no software. Como resultado, o programa pode não encontrar os arquivos necessários para funcionar.

3.1.7 Furto digital mediante fraude

Os crimes definidos como fraude virtual, estão inseridos entre os crimes digitais mais comuns, por sua facilidade, onde não há necessidade de conhecimento avançado sobre computadores, podendo ser aplicado por qualquer um.

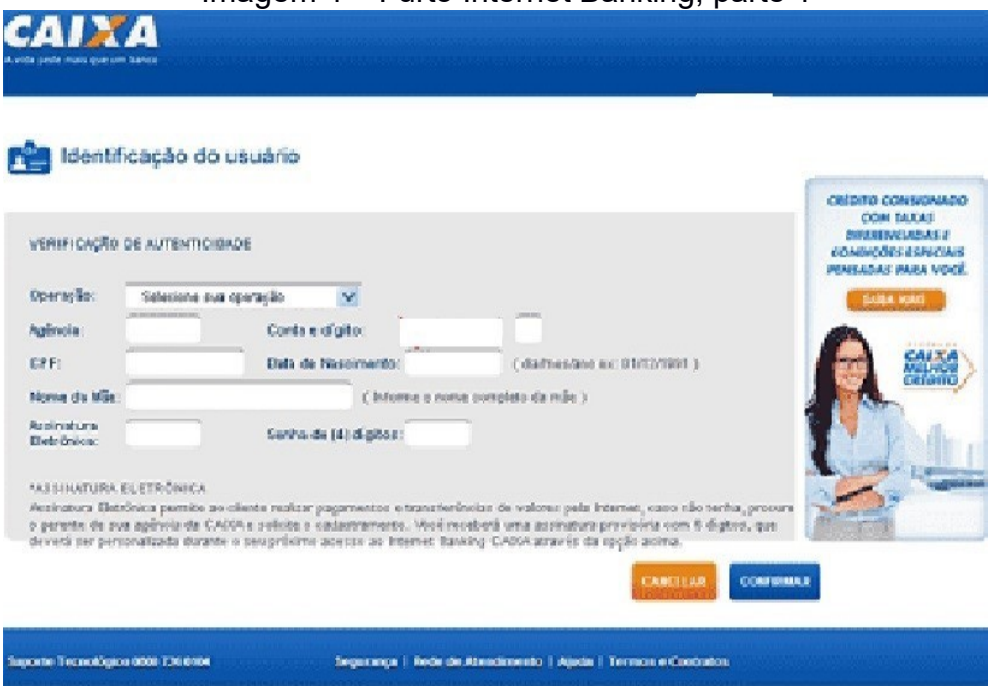
Desde muito tempo, pessoas más intencionadas usam métodos fraudulentos para obter vantagem para si ou outrem, fazendo com que a vítima sofra algum tipo de prejuízo. Peck (2016) diz que:

> Toda fraude, independentemente da sua natureza, tem como pressuposto a utilização de um subterfúgio para ludibriar a vítima, seja por meio da ação ou da omissão do agente, isto é, o fraudador fornece informação errônea a vítima ou ainda omite.

A fraude eletrônica se dá a uma ação prejudicial e intencional a uma vitima, causada por procedimentos e informações, de propriedade de pessoa física, ou jurídica, com o objetivo de alcançar benefício, ou satisfação psicológica, financeira e material".Nessa lógica, o criminoso envia uma mensagem que não foi solicitada (e-mail falso), passando-se por uma instituição financeira, uma empresa ou um banco conhecido, através de um perfil falso na internet, com objetivo de obter dados da vitima, para que assim possa ter acesso aos valores mantidos pela instituição, sem ser pegos pelo sistema de vigilância e proteção. financeira sobre os valores mantidos a sua guarda. Podemos ver que há divergência na doutrina em relação a que artigo o delito de fraude eletrônica se enquadraria, 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." ou 155 "subtrair, para si ou para outrem, coisa alheia móvel: § 4º - A pena é de reclusão de dois a oito anos, e multa, se o crime for cometido: I - com abuso de confiança, ou mediante fraude, escalada ou destreza", ambos do Código Penal.

Abaixo pode-se observar um dos meios usados para obter dados do cartão de crédito da vitima. Cumpre lembrar que embora parecidos, esse crime não deve ser confundido com o de estelionato, pois no estelionato o criminoso procura obter o consentimento da vítima para a pratica o ato ilícito e no furto sua qualificadora é utilizada para burlar a esfera de vigilância da vítima, como explicado anteriormente. Veja:

Imagem 4 – Furto Internet Banking, parte 1



Fonte: <seumicroseguro.com>

Imagem 5 – Furto Internet Banking, parte 2

Fonte: <seumicroseguro.com>

3.1.8 Estelionato Digital

O estelionato digital é um dos crimes mais praticados do nosso ordenamento jurídico, esta previsto no art. 71, do Código Penal que dispõe:

> 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, de1 (um) a 5 (cinco) anos, e multa.

Esse tipo de crime faz com que a vítima entregue a coisa por livre e espontânea vontade, sendo comum um estelionatário utilizar condutas típicas tal como encaminhar um e-mail com um conteúdo falso, induzindo a vitima a acreditar e acessar ao link enviado, direcionando para um site confiável com o intuito de

atualização de seus dados, podendo assim o criminoso ter acesso as informações pessoais e adquiri-las. Na grande maioria, essa pratica é feita para obter informações de dados bancários.

Tendo em vista que o crime de estelionado digital e delito de furto mediante fraude virtual, são parecidos e fácil de confundi-los, houve a necessidade de diferencia-los, existindo atualmente a pacificação nas doutrinas e jurisprudências acerca do crime de estelionato.

Essa explicação jurisprudencial foi dada através do Conflito Negativo de Competência 67343 GO 2006/0166153-0, pela Ministra Laurita Vaz, da Terceira Seção do STJ, o qual dispõe a seguinte explicação:

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

3.1.9 Extorsão

Neste tópico será analisado o delito de extorsão no meio digital, criado com o objetivo de infiltrar-se em sistemas sem a percepção de seu titular. Procuram criptografar os dados com senhas da vitima, bloqueando seu acesso e, em muitos casos, inutilizando o dispositivo infectado e para que a vítima recupere o controle de seu dispositivo ou arquivos infectados, ela deve realizar um pagamento. SAISSE (2016) explica que:

> O ransomware é propagado das mais variadas formas, seja por intermédio de acesso aos sites suspeitos que liberam o código malicioso apenas com a visita do usuário ou por arquivos disfarçados (músicas, imagens, etc.), normalmente divulgados em redes sociais ou enviados por e-mail aparentando algo comum, de interesse público, cobranças, causas sociais, etc. Ainda podem ser liberados via instalação de aplicativos vulneráveis em dispositivos móveis ou computadores.

Os criminosos operam sem o conhecimento do usuário, com a finalidade de instalar todos seus sistemas bloqueio na maquina da vitima. Finalizado esse processo, os delituosos exibem mensagem ou imagens para a vitima informando o bloqueio dos dados e do resgate a ser pago para liberação, sendo totalmente inacessíveis os dados do dispositivo.

Na maioria das vezes, os maiores alvos para esse tipo de crime são, dispositivos de usuários individuais, redes corporativas e até mesmo do governo também são afetadas. A chance de perder esses dados são enormes, sendo assim, consequentemente a vitima paga aos criminosos o valor exigido para recuperação dos dados. Como afirma SAISSE (2016) “isso impulsiona a economia clandestina e como resultado aumentam o número de novos criminosos e o número de ataques.”.

Sendo aplicado o art. 158, do Código Penal, que dispõe:

> Art. 158 - Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa.

Nesse tipo de crime a vítima sabe o que está acontecendo e faz a entrega da coisa contra a sua vontade, em razão de violência ou grave ameaça.

4. LEGISLAÇÃO NACIONAL APLICÁVEL

Podemos dizer que atualmente, a legislação vigente no Brasil já abrange os principais crimes virtuais, mesmo não exemplificando separadamente, os artigos do Código Penal já tipificam as mesmas condutas, portanto podemos aplica-las ao caso. Como exemplo, o artigo 139 do Código Penal, prevê a pena de detenção de 3 meses a 1 ano e multa pelo crime de difamação, o fato de imputar a alguém fato ofensivo a sua reputação, sendo punido de igual forma o crime cometido no âmbito virtual.

Contudo, seria de extrema importância a existência de uma lei especifica que garantisse maior efetividade do judiciário no combate aos crimes virtuais. Sendo assim, em 2012, com a entrada em vigor das Leis 12.735 e 12.737, a possibilidade de responsabilização do agente e daqueles que invadem dispositivos para roubar dados se tornou mais concreta.

A Lei 12.735, art. 4° e 5°, veio regulamentar a ação da polícia judiciária, que dispõe:

> 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;

Ocorreu varias críticas a essa lei pelo evidente retrocesso legislativo em comparação à Convenção de Budapeste, que vamos tratar mais adiante.

Diante disso surgiu uma urgência constitucional na criação do Marco Civil da Internet.

Já durante a criação da Lei 12.737, ocorreu o incidente com a atriz Carolina Dieckmann, que teve seu dispositivo invadido e fotos íntimas de seu computador divulgadas, e desde então a lei ficou conhecida carregando seu nome. Esta lei visa tipificar condutas que ate então não eram tratadas como infração penal, como os

delitos a respeito de invasões a dispositivos informáticos, da interrupção ou perturbação de serviço telegráfico, telefónico, informático, telemático ou de informação de utilidade pública e da falsificação de documento particular e cartão.

Porém, ocorreu descontentamento por uma grande parte, devido ao motivo de baixas penas atribuídas a essa infração. Também, tais leis não atingiu toda a necessidade de especificar as diferentes formas de delitos. Repara-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 observar, a lei prevê que a invasão aos 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, em que o agente tem por intuito acessar apenas os dados para proveito próprio ou para chantagear a vítima, ou também nos casos em que o delituoso distribui esses arquivos roubados. Então, se o agende não violar esses dispositivos de segurança acima, não terá cometido nenhum crime.

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 podemos fazer analogias e interpretações em desfavor do réu.[34]

A Lei 12.965 sancionada em 2014, conhecida como Marco Civil da Internet, que visa regulamentar o uso da Internet por meio de garantias, princípios, direitos e deveres aos usuários. Essa ideia surgiu com a resistência à Lei de Azeredo (12.735/12), que foi uma proposta do Poder Executivo a Câmara dos Deputados e aprovada em 23 de abril de 2014, com o intuito de regular a utilização, garantir a privacidade, a inviolabilidade da vida privada, bem como garantir o devido uso da internet. É regida a partir de princípios como os da neutralidade, da reserva jurisdicional, da responsabilidade dos provedores, dentre outros. Foi de extrema importância para que possa impor as obrigações e responsabilidades aos usuários e provedores.

5. LEGISLAÇÃO INTERNACIONAL E TRATADOS

Nesse tópico, podemos citar a Convenção de Budapeste, conhecida também como Convenção do Cybercrime, que se trata de um tratado internacional de direito penal e processual surtido na União Europeia em 2001 e aderido por diversos países. E desde então, visam criar uma política criminal, com intuito proteger a sociedade contra a criminalidade na era tecnológica através de legislação e cooperação internacional.

Podemos identificar que ela trata de tipificar os crimes que envolvem pedofilia; as infrações relacionadas aos crimes com computadores; os crimes virtuais como infrações de sistemas e também tipificar violações de direitos autorais. Ela trata também da cooperação internacional e da competência, deixando que as partes decidam a jurisdição mais apropriada para o procedimento legal.

> Artigo 22º - Competência
>
> 1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer a sua competência relativamente a qualquer infração penal definida em conformidade com os artigos 2º a 11º da presente Convenção, sempre que a infracção seja cometida: a) No seu território; ou b) A bordo de um navio arvorando o pavilhão dessa Parte; c) A bordo de uma aeronave matriculada nessa Parte e segundo as suas Leis; ou d) Por um dos seus cidadãos nacionais, se a infração for punível criminalmente onde foi cometida ou se a infração não for da competência territorial de nenhum Estado.[35]

Para que possamos aprofundar o entendimento, é valido compreender como funciona a Cooperação Internacional.

A ONU (Organização das Nações Unidas) tem por objetivo incentivar os países a criarem tratados bilaterais e multilaterais, para que se possa aumentar a eficácia dessas cooperações, ampliando as bases jurídicas e preenchendo com bases legais em que os países podem contar, procurando harmonizar as políticas de

colaboração entre os países em âmbito penal, de forma que consiga estabelecer regras para o combate de crimes transnacionais.

Outro fato importante é a resposta ao pedido de cooperação internacional, que significa que os países devem atender as solicitações de outros países para investigar e tomar providencias cabiveis aos crimes transnacionais. Para que isso ocorra, fica a mercê da infraestrutura, dos profissionais e das possibilidades que o país tem para que possa atendê-las. Geralmente as autoridades designadas para tais atividades são os ministérios da Justiça, procuradorias-gerais e ministérios de Relações Internacionais, sendo eles preparados para que desempenhem essa função.

6. COMPETÊNCIAS PARA PROCESSAR E JULGAR

Para que possamos abordar o conceito de jurisdição, de forma essencial, que significa ser o poder que o Estado concede ao Juiz para que ele possa aplicar o direito no caso concreto, aplicando assim uma lei a cada caso. A competência, assim como o Estado concede poder ao Juiz de dizer o direito, limitando o poder, ou seja, a competência é o limite da Jurisdição do Juiz. A competência é a área de atuação do juiz.

Os crimes virtuais podem ser atuados em qualquer lugar do mundo que tenha acesso à internet e esse acesso pode ser feito não somente através de computadores, mas também pelos smartphones, televisores e demais equipamentos informáticos/eletrônicos. Devido a mobilidade dos equipamentos informáticos, acaba se tornando complexo para determinar qual juiz é competente para julgar, e ainda não há legislação que norteie estes casos.

Nos casos desses crimes praticados no Brasil, o Código de Processo Penal Brasileiro dispõe 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 iniciaram no Brasil, mas progrediram para fora, são de competência da Justiça Federal.

A lei 7.209 de 11 de julho de 1984 no seu artigo 5º e 6º dispõe 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, é de suma importância observar onde ocorreu os fatos criminosos daqueles crimes cometidos pela Internet, e caso tal local não consiga ser identificado, a competência ficará a cargo do Juízo que iniciou as investigações.

Havendo a hipótese de transnacionalidade do crime virtual, este será de competência da Justiça Federal.

CONCLUSÃO

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.

O principal objetivo da presente monografia foi compreender os crimes virtuais junto a evolução tecnologia e a ótica da Legislação Brasileira.

Contudo, podemos constar a grande dificuldade de delinear o espaço virtual e sua fronteira, tendo em vista que a evolução tecnológica tem se expandido cada vez mais, e consequentemente surgindo diversos tipos de delitos cibernéticos.

Esses crimes exigem bastante atenção, uma vez que a internet se tornou essencial na vida em sociedade, necessitando de normas que regulem as ações humanas no ambiente virtual.

No segundo capítulo analisamos o surgimento desses delitos junto ao Direito, onde veio a necessidade do Direito direcionar seu olhar voltado para a internet, junto com a Constituição Federal.

No terceiro capítulo conceitua-se o crime virtual, mostrando quem são os cibercriminosos e de que maneira ocorre esse tipo de crime. Desconceitua também o paradigma social de que o cibercriminoso é necessariamente alguém com conhecimento técnico, mas que pode ser também um usuário comum que utiliza a internet e pratica condutas tipificadas no Código Penal.

A falta de legislação também se mostra um problema, como no exemplo do canibalismo citado anteriormente neste trabalho. Não se admite a falta de norma que proíba tal prática apenas porque o fato é esporádico. Nota-se que a falta de informação é um dos motivos para que a sociedade permaneça inerte às brutalidades que são comandadas.

Se faz necessária também a criação de normas específicas que englobem de maneira mais eficaz os atos cometidos na esfera virtual, afinal, por mais que o legislador tenha criado leis para tanto, observa-se deficiências quanto a efetividade da norma, onde podemos ver que a legislação brasileira não consegue acompanhar os avanços tecnológicos com a mesma agilidade que é oferecida pela

internet, porém as leis existentes ainda se aplicam aos casos discutidos na pesquisa, devendo apenas regulamentar questões especificas, como é o caso do Cyberbullying.

No quarto capitulo, conceitua-se as competências para processar e julgar os crimes virtuais.

Aborda também nos últimos capítulos, a maneira como as legislações nacionais e internacionais se posicionam a fim de repelir condutas criminosas. Evidencia-se que a promulgação do marco civil da internet mostrou-se de papel fundamental para regular a utilização da internet, juntamente à Convenção de Budapeste.

Conclui-se também que a Cooperação Internacional é essencial no combate aos cybercrimes, assim como as convenções entre países que visam harmonizar a atividade e os seus ordenamentos jurídicos.

Cabe ressaltar que a reflexão acerca do tema visa que o Direito Penal alcance de forma mais plena as mudanças que a sociedade vem sofrendo frente à evolução das ciências tecnológicas, a fim de torná-lo concomitante com a realidade fática social.

REFERÊNCIAS

ADOLESCENTES. Jornada estadual contra a violência e a exploração sexual de criança e. **Seis livros sobre abuso e exploração de crianças**. Disponível em: <http://wp.clicrbs.com.br/jornadasestaduais/2014/05/28/6-livros-sobre-abuso-e-exploracao-da-crianca/>. Acesso em 10 dez. 2019.

BARRETO, Alessandro Gonçalves. **Investigação Digital em fontes abertas**. Rio de Janeiro. Brasport, 2017.

BRASIL, **Constituição Federal**: Lei nº 9.296, 24 de julho de 1996. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/L9296.htm>. Acesso em: 26 nov. 2019.

BRASIL, **Código Penal**: Decreto-lei nº 2.848, de 07 de dezembro de 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737 .htm>. Acesso em: 05 nov. 2019.

BRASIL. Lei nº 12.735, de 30 de nov. de 2012**. Para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.** Brasília, DF, 30 nov. 2012.

BRASIL. Lei nº 12.737, de 30 de nov. de 2012. **Tipificação criminal de delitos informáticos**. Brasília, DF, 30 nov. 2012.

BRASIL. Safer Internet Center do: **Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos**. Disponível em: <http://indicadores.safernet.org.br/index.html>. Acesso em: 03 nov. 2019.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas reais**. Rio de Janeiro: Brasport, 2014.

COLLI, Maciel. **Cibercrimes:** Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos. Curitiba: Juruá Editora, 2010.

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

FILHO, Adilson Paulo Prudente do Amaral (2011). **Crimes cibernéticos:** e o grupo de combate da procuradoria da República no estado de São Paulo. REVISTA JURÍDICA CONSULEX, nº 343, p. 37-38, maio 2011.

FIORILLO, Celso Antônio Pacheco. **Crimes no meio ambiente digital**. 1 Ed. São Paulo: Saraiva, 2013.

GRECO, Rogério. **Código Penal comentado**. 11 Ed. Rio de Janeiro, 2017, p. 755.

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

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

LINS, Bernardo Felipe Estelita. **A evolução da internet**: uma perspectiva histórica. In cadernos ASLEGIS, nº 48. Brasília: ASLEGIS, 2015.

MASSON, Cleber. **Direito penal esquematizado**: parte especial. 6. Ed. São Paulo: Método, 2016.

NOW, IDG. **Tuites com conteúdo racista de Mayara**. Disponível em: <http://idgnow.com.br/internet/2011/12/12/ministerio-publico-aceita-denuncia-e-mayara-petruso-respondera-por-racismo/>. Acesso em: 10 nov. 2019.

NUCCI, Guilherme de Souza, **Código Penal Comentado**, 16. Ed. Rio de Janeiro: Forense, 2016.

RAMALHO, José Ricardo. **Pedofilia e a rede do mal:** os aspectos legais e punitivos relacionados ao uso da internet para a prática de crimes sexuais contra crianças e adolescentes. REVISTA VISÃO JURÍDICA, nº 343, p. 28-35, 12 dez. 2019

RODRIGUES, Guilherme. **Injúria racial contra filha de Gio Ewbank**. Disponível em: <https://observatoriodatelevisao.bol.uol.com.br/famosos/2016/11/de pois-de-ofender-gaby-amarantos-internauta-ataca-filha-de-bruno-gagliasso-parece-uma-macaquinha>. Acesso em: 10 nov. 2019.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. 1. Ed. São Paulo: Memória Jurídica, 2004.

SAISSE, Renan Cabral. **Ransomware: "sequestro" de dados e extorsão digital.** Disponível em: <http://direitoeti.com.br/artigos/ransomware-sequestro-de-dados-e-extorsao-digital/#_edn4>. Acesso em: 11 dez . 2019

SANTOS, Coriolano Aurélio de Almeida Camargo; FRAGA, Ewelyn Schots. **As Múltiplas Faces dos Crimes Eletrônicos e dos Fenômenos Tecnológicos e Seus Reflexos no Universo Jurídico**. São Paulo: OAB SP, 2010.

SILVA, Ana Beatriz Barbosa. **Bullying: mentes perigosas nas escolas.** Rio de Janeiro: Objetiva, 2010.

SOARES, Luís Eduardo. **PEC - 51: revolução na arquitetura institucional da segurança pública**. In: Boletim do IBCCrim, ano 21, nº 252, novembro de 2013. São Paulo ZEVIAR-GEESE, G. **The State of the Law on Cyberjurisdiction and Cybercrime on the Internet. California Pacific School of Law**. Gonzaga Journal of International Law. Volume 1. 1997-1998.

SEGURO, Seu micro. **Furto internet banking**. Disponível em:<https://seumicroseguro.com/2014/04/07/site-da-caixa-possibilitou-ataques-de-phishing/>. Acesso 10 dex. 2019.

TÁVORA, Nestor. ALENCAR, Rosmar Rodrigues. **Curso de Direito Processual Penal.** 12. Ed. Bahia: JusPodivm, 2017, pág. 387.

ZANIOLO, Pedro Augusto. **Crimes Modernos**: o impacto da tecnologia no Direito. 3 Ed. 2016. Curitiba. Juruá Editora.