CENTRO UNIVERSITÁRIO DR. LEÃO SAMPAIO – UNILEÃO CURSO DE
GRADUAÇÃO EM DIREITO

ANA LAURA MIRANDA ALENCAR LÓCIO

ENTRAVES DA APLICAÇÃO DA LEI PENAL NOS CRIMES VIRTUAIS.

Juazeiro do Norte

2019

ANA LAURA MIRANDA ALENCAR LÓCIO

ENTRAVES DA APLICAÇÃO DA LEI PENAL NOS CRIMES VIRTUAIS.

Monografia apresentada à Coordenação do Curso de Graduação em Direito do Centro Universitário Dr. Leão Sampaio, como requisito para a obtenção do grau de bacharelado em Direito.

Orientador(a): Prof. Francisco Thiago da Silva Mendes

Juazeiro do Norte

2019

ENTRAVES DA APLICAÇÃO DA LEI PENAL NOS CRIMES VIRTUAIS

Ana Laura Miranda Alencar Lócio¹
Francisco Thiago da Silva Mendes²

RESUMO: O Presente trabalho irá buscar o entendimento sobre as dificuldades e como superar esses problemas que a ciência do Direito tem na hora da aplicação de suas normas quando se encontra em um delito praticado por meios eletrônicos e em suas plataformas. Para isso, deverá analisar as situações que englobam o uso da internet e os crimes que possuem mais ocorrência nesse meio virtual. Por isso, deverá passar uma linha horizontal referente à sua história e quais os conceitos de crime virtual. Em seguida, deverão analisar quais são esses crimes e o motivo da dificuldade que o Direito tem da aplicação de suas normas para poder efetivar a finalidade da pena referente à repressão dessas condutas ilícitas virtuais. Nesse caso, essa pesquisa foi realizada por meio do método dedutivo seguindo um levantamento bibliográfico, na qual obteve como respostas que a inaptidão que o Estado vem tratando os crimes cometidos no espaço virtual por meio de lacunas legislativas, tanto no ponto de vista de criar leis próprias sobre a temática quanto sobre o modelo de qualificadora ou até mesmo como causa de aumento de pena, a fim de trazer uma maior segurança jurídica e social.

Palavras-chave: Crime virtual. Direito virtual. Plataforma cibernética.

ABSTRACT: This paper will seek understanding of the difficulties and how to overcome these problems that the science of law has when applying its rules when finding an offense committed by electronic means and its platforms. To do so, analyze how situations involving the use of the Internet and the crimes that have more occurrence in this virtual environment. Therefore, you can pass a horizontal line referring to your history and what are the concepts covered about who is a virtual crime. Then analyze what these crimes are and the reason for the difficulty or the right to enforce the rules in order to enforce a punishment for the prosecution of these virtual illicit practices. In this case, this research was conducted through the deductive method following a bibliographic survey, in which it obtained as answers that the inability that the State has been treating crimes committed in the virtual space through legislative gaps, both from the point of view of creating laws own on the subject as the qualifier model or even as a cause of increased penalty, in order to bring greater legal and social security.

Keywords: Virtual crime. Virtual law. Cyber platform.

1 INTRODUÇÃO

¹Discente do curso de Direito da UNILEÃO. E-mail: analauramalocio@hotmail.com

²Docente do curso de Direito da UNILEÃO. E-mail: thiagomendes@leaosampaio.edu.br

O presente trabalho se trata de um tema atual e bastante discutido pela população, se faz necessário estudar os principais crimes que vem sendo cometidos em face do mundo virtual e mostrar a relevância dessas condutas serem tipificadas legalmente, pois na sua ausência, tratará uma lacuna legislativa, como também uma crise social, pois acaba por se mostrar como forma de incentivar a prática dessas condutas, ocasionando na dificuldade da aplicação do poder-dever de punir do Estado, devido à falta de previsão legal.

As Tecnologias de Informação Comunicação (TIC) revolucionaram a sociedade nos últimos anos. Os hábitos e a forma de vida da humanidade evoluíram junto com essas transformações que são evidentes e se fortalecem a cada dia, levando uma intensa interferência em todos os campos da vida social, trazendo como consequência que o mundo virtual está convivendo com o mundo real, pois a TIC se encontram por todos os lugares, formando-se a era dos bytes.

Por isso, diante da função principal, cabe à ciência do Direito acompanhar as mudanças da sociedade e caminhar junto com ela para que se torne eficaz a sua função, principalmente quando se trata de Direito Penal que somente irá configurar uma conduta como delituosa se estiver prevista em lei, conforme presente no princípio da legalidade.

Por isso é evidente a necessidade da ciência jurídica do Direito se adaptar-se a essa nova realidade que não pode mais ser desprezada, pois as evidentes consequências da utilização da informática e da internet no mundo jurídico se torna algo indiscutível e que deve ser tratado de acordo com a sua peculiaridade.

Essa situação se torna algo incontestável, por exemplo, quando por meio de uma tela do microcomputador ou pelo próprio telefone, o ser humano tem a possibilidade realizar diversos negócios jurídicos em um curto espaço de tempo e sem a necessidade de se deslocar do local em que se encontra ou do local que escolheu para tal empreitada, tendo toda essa ação realizada pelo ciberespaço, plugado na internet.

Com abertura da nova era digital, o ser humano está cada vez mais inserido no uso de tecnologia na sua diária, sendo esse tipo de situação cada vez mais incorporada pela a população por meio da internet e de suas ferramentas, iniciando, assim, as relações no mundo virtual. Porém, por muitas vezes, alguns desses indivíduos passam a visualizar esse novo universo como uma terra sem lei.

Para aqueles que acreditam que por se apresentar em um ambiente aberto virtual, não será abrangido pela a lei, levando os seus usuários a prática de atos ilícitos nesse ambiente, pois acreditam que não chegaram a ser punidos nesse âmbito.

Diante disso, o presente trabalho buscar abordar essa temática e seus advenços para que possa compreender a importância de entender que assim como nos crimes tradicionais, os crimes realizados no ambiente virtual devem ser tratados como um tema atual, pois os mesmos podem ocorrer a qualquer tempo e qualquer lugar e ter seu conteúdo espalhado muito facilmente.

Por isso, será realizada uma pesquisa com base nos principais autores que discorrem sobre esse tema, através do método dedutivo, utilizando pesquisas bibliográficas de artigos e livros que tratam sobre crimes virtuais, na qual abordará sobre a evolução histórica, bem como o conceito sobre crimes cibernéticos e como o Direito vem tratando essa temática e quais os crimes mais cometidos no universo virtual.

Diante disso, tomaremos como finalidade principal se trata de uma investigação sobre os entraves e desafios para aplicação da lei penal nos crimes virtuais, partindo das premissas de analisar a historicidade dos crimes virtuais, verificar a inaptidão da legislação atual sobre os crimes virtuais e examinar os entraves e desafios da repressão aos crimes virtuais.

Logo, a problemática do presente trabalho gira em torno da ausência de provisão legal específica referente ao tema dos delitos cibernéticos, bem como as lacunas presentes nas normas legais que já tratam a cerca dessa situação, trazendo uma dificuldade na aplicação processual dessa situação, ou seja, demonstrando a omissão estatal para elaborar e aplicar leis que circulem o tema dos crimes cibernéticos.

2 METODOLOGIA

O método de pesquisa que será empregado na presente artigo será o método dedutivo, pois seguirá uma linha de raciocínio básica, na qual irá primeiro analisar a história do surgimento dos crimes virtuais no Brasil, bem como a evolução legislativa sobre esses fatos e o conceito de crimes virtuais.

Diante disso, essa pesquisa irá se desenvolver por meio de uma pesquisa teórica referente ao assunto de crimes virtuais, seguindo um levantamento bibliográfico, revistas físicas e virtuais, bem como artigos e demais recursos que serão necessários durante a pesquisa.

3 A HISTORICIDADE DOS CRIMES VIRTUAIS

Os crimes virtuais, também chamados de crime informático, crime cibernético, e-crime, cyber crime, crime eletrônico ou crime digital, são condutas delituosas praticadas por pessoas que se utilizam dos meios digitais, seja ele de comunicação ou não, para efetuar condutas ilegais, acreditando que por se encontrar em um universo virtual, não serão atingidos pela égide do Direito.

Os primeiros usos da internet foram datados em 1969 como um meio do governo dos Estados Unidos durante o período de guerra fria. Esse procedimento foi conseguido por meio da ARPA (Advanced Research Projects Agency), que se empenhou em conseguir uma maneira segura e fácil de conexão entre computadores para compartilhar informações de hardware e software.

Diante disso, a internet teve sua formação para ser utilizado como forma de arma Norte Americana para distribuição de informações para a suas bases, ou seja, consistia em uma maneira eficaz de ligar todas as centrais de computadores das bases militares estratégicas para em caso de um suposto ataque Russo, o mesmo ser comunicado aos demais de forma mais rápida ou para caso uma das bases militares fossem atacadas, as outras poderiam permanecer com o seu funcionamento de forma autônoma, fazendo com que aquele ataque não prejudicasse as operações militares que estavam ocorrendo.

A Internet somente chegou ao Brasil durante o período de 1988 por meio da iniciativa das comunidades acadêmicas de São Paulo e do Rio de Janeiro, na qual foi instituído em 1989, a Rede Nacional de Pesquisa, pelo Ministério de Ciência e Tecnologia, objetivando que houvesse uma maior disponibilidade de serviços de acesso a Internet.

Logo, a era digital vem avançando e atingindo cada vez mais um maior número de usuários no mundo, trazendo um grande avanço nas interações humanas, ou seja, a internet é vista como um salto no desenvolvimento tecnológico e, consecutivamente, um salto no desenvolvimento humano, que vem ocasionando uma mudança de paradigma da maneira em que o ser humano irá interagir e agir no seu meio social. Todavia essa situação está sendo corroída por usuários que encaram essa tecnologia como um meio de conseguir ofender um bem jurídico tutelado pelo Estado.

O desrespeito a um bem protegido pelo o Estado por intermédio da internet ou qualquer outro meio no Cyber espaço, configura-se como crime virtual. Para Rossini, a definição de delito informático é tratada como:

Aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda,

direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade. (ROSSINI, 2004.)

Nesse mesmo sentido a autora Maria Helena Junqueira Reis explica o delito eletrônico como:

“O delito eletrônico no seu sentido amplo é configurado como qualquer conduta criminogena ou criminal em cuja sua realização haja emprego da tecnologia eletrônica como método, meio ou fim, já no seu sentido estrito é configurado como qualquer ato ilícito penal em que computadores, suas técnicas e funções desempenham um papel como método, meio ou fim.” (Reis, 1997.).

Seguindo uma linha tênue sobre o conceito de delito eletrônico apresenta-se a perspectiva referente ao entendimento de Maria de La Luz Lima presente na seguinte citação:

Delito eletrônico, em sentido amplo, é qualquer conduta criminogena ou criminal em cuja realização haja o emprego da tecnologia eletrônica como método, meio ou fim, em um sentido estrito, qualquer ato ilícito penal em que os computadores, suas técnicas e funções desempenham um papel como método, meio ou fim. (LIMA, 2003)

Nesse mesma linha de raciocínio, a referida autora passou também a utilizar uma divisão dessa definição em três tipos de categorias listadas a baixo:

I) Aqueles que utilizam a tecnologia eletrônica como um método, ou seja, condutas criminais onde os indivíduos utilizam métodos eletrônicos para atingir o seu resultado ilícito;

II) Aqueles que utilizam a tecnologia eletrônica como um tipo de meio, ou seja, condutas criminais em que para a realização de um delito utilizam o computador como meio;

III) Os que utilizam a tecnologia eletrônica como fim, ou seja, condutas dirigidas contra a entidade física do objeto ou máquina eletrônica ou seu material com o objetivo de danificá-lo.

Também é importante mencionar que o Direito Internacional deslumbrou sobre a temática dos crimes virtuais, tal como na conceituação incorporada durante o Oitavo Congresso sobre Prevenção de Delito e Justiça Penal, ocorrido em Havana, Cuba, em 1990, na qual a Organização das Nações Unidas (ONU) publicou um relatório sobre os delitos informáticos, na seguinte maneira:

1. Fraudes por meio de manipulação de computadores, configurada por meio de manipulação de dados de entrada, ou manipulação de programas, ou manipular dados de saída, falsificando uma característica do seu sistema, ou por meio da manipulação informática, técnica especializada que aproveita as repetições automáticas dos processos do computador.

2. Falsificações informáticas no seu objeto, por exemplo, quando se alteram dados de documentos presentes em um computador ou no seu instrumento, quando o computador é o meio para realizar a falsificações de documentos, seja criando ou modificando informações.
3. Por meio de danos ou modificações de programas ou dados, por exemplo, através da modificação, sem autorização, de programas de informática com o intuito destruir ou degradar o funcionamento normal do sistema, por meio de elementos como o vírus. (ONU, 1990)

No que diz respeito à evolução da internet em se tornar uma ferramenta cada vez mais presente na vida das pessoas, o poder legislativo propôs a criação da lei 12.965/14, conhecida como o Marco Civil da Internet, que passasse a regular o funcionamento da internet para que seu uso não ocorresse de forma desenfreada. Essa lei trouxe um relevante interesse para sua elaboração, fazendo com que antes de discutir o quórum para se tornar uma lei, fosse encaminhada para a Secretaria de Assuntos Legislativos do Ministério da Justiça, bem como a ocorrência de audiências públicas em todo o país.

Essa lei buscava estabelecer princípios e garantias para que a utilização da internet ocorresse de forma livre e democrática. Nessa situação, foram criados direitos e deveres para os seus usuários no intuito de estabelecer uma harmonia durante o uso da internet, como na proteção e privacidade de dados dos usuários, salvo nas investigações criminais.

Esses tipos de delitos podem ser praticados por qualquer pessoa, ou seja, se tratam de um crime comum. Todavia, na configuração do sujeito ativo desses delitos tem ganhado um maior destaque os sujeitos conhecidos como hacker e cracker tendo uma diferenciação significativa conforme apresenta Plantullo em seu livro “Estelionato eletrônico”, na qual os primeiros são pessoas que apresentam um vasto conhecimento sobre a programação de um computador e utilizam dessa situação para a prática de ilícitos relacionados à criação ou alteração de sistemas de informática. Enquanto os cracker são aqueles que utilizam dos seus conhecimentos sobre informática para a prática de atos ilícitos, por meio de invasão e deterioração de sistema para roubar informações, por exemplo, na prática de transação bancária fraudulenta. Nesses termos o presente autor especificou como:

Hacker são pessoas dotadas de amplo conhecimento de programação e utilizam este conhecimento para o lícito, criando ou melhorando sistemas e buscam superar seus próprios limites. Cracker são pessoas também dotadas de grande conhecimento de programação, mas utilizam este conhecimento para atividades ilícitas, invadindo e destruindo sistemas, roubando informações, praticando transações bancárias fraudulentas, chantageando, extorquindo e toda série de infrações ao direito alheio. (Plantullo, 2003)

Com isso, percebe-se que os crimes virtuais possuem uma dimensão vasta na sua conceituação criminal, pois se tratam de condutas que se encaixam perfeitamente no conceito

analítico de crime, por se tratar de uma conduta ilícita, antijurídica e culpável, tendo apenas como peculiaridade por se tratar de um crime cometido em um universo virtual. Assim como acentua Fabrício Rosa (2002, p. 53-54), conforme transcrita a baixo;

É a conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; 2. O „Crime de Informática“ é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. Assim, o Crime de Informática“ pressupõe dois elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrá-los; 4. A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5. Nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc. (Rosa, 2002).

Ao observar essa integração que cresce através da tecnologia, principalmente da internet e das redes sociais, cria-se uma nova plataforma de relação social, que se apresenta em um fluxo intenso de usuários e informações a um simples toque em um pequeno espaço de tempo. Porém, o começo da problemática desse meio se apresenta, por exemplo, quando ocorre a discursão entre a possibilidade do anonimato decorrente do direito da privacidade e da liberdade em face dos demais direitos fundamentais presentes na Constituição Federal, trazendo diversos desafios para o aplicador do Direito, pois é necessário descobrir o limite de cada direito quando se insere em um mundo virtual. Afinal, o direito de uma pessoa se inicia quando o do outro se acaba.

No que se refere ao ordenamento jurídico interno do Brasil, a privacidade é tratada em sua tutela fundamental no artigo 5º em seus incisos X e XII da Constituição Federal³, na qual

³ **Art. 5º, CF/88:** Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

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; (Brasil, 1988)

apresenta que se constituem como direitos dos cidadãos brasileiros a proteção da vida privada, da intimidade e a inviolabilidade dos sigilos de correspondência, das comunicações telegráficas, de dados e das comunicações telefônicas. Todavia, para saia do mundo abstrato e se insira no mundo concreto é necessário também observar outros dispositivos legais presentes na Constituição Federal (Brasil, 1988).

Para isso, o ordenamento jurídico brasileiro apresenta como seu vetor principal o princípio acerca da proteção da pessoa humana e a sua privacidade como forma de um direito fundamental, com isso garante que independente do direito que se enquadra no caso concreto, esse direito somente vai ser válido se respeitar o princípio da dignidade da pessoa humana, tal entendimento também deve ser observado quando se trata da utilização da plataforma virtual, pois garante uma relação harmoniosa e respeitável entre seus diversos usuários, garantindo, portanto, uma paz social no âmbito virtual conforme exigido no mundo real.

Logo, os direitos e deveres presentes nas sociedades digitais não podem deixar de existir fora dela e vice-versa. Pois, uma pessoa que ataca a outra com palavras racistas na internet, por exemplo, será responsabilizada civilmente por indenização moral e criminalmente por crimes contra a honra ou o próprio delito de racismo devido as suas próprias ações nesse meio virtual. Tal como ocorre no caso de utilização da internet para cometer diversas fraudes e criar golpes com o intuito de prejudicar alguém dentro do mundo digital, entre outros diversos crimes que se apresentam cada vez mais na esfera virtual.

A internet, portanto, trata de um grande marco da história da humanidade. Essas novas ferramentas ocasionam transformações significativas da forma como a humanidade se comporta, ao passo que o uso livre da internet faz com que os usuários enxerguem esse meio como uma plataforma em que não existe limite na sua atuação. Porém essa situação pode trazer perplexidade por parte das pessoas, que ainda não entendem como se deve comportar-se nesse "segundo mundo de ação humana", popularmente conhecida como "cyber espaço". Diante disso, ficou uma concepção errada de que a internet deveria ser tratada como "terra sem lei", onde tudo seria permitido pela falsa percepção de que é impossível a descoberta da verdadeira identidade da pessoa.

Tal fato gerou uma observação que estava havendo uma deficiência dos meios utilizados pelo direito penal tradicional no combate à criminalidade virtual que estava cada vez mais presente na vida das pessoas conforme a internet ia crescendo. Com isso os Códigos Penais e legislações penais especiais foram atingidos por essa nova forma de vida que a

internet e o uso de tecnologia estão gerando, porque o direito penal está entrelaçado da soberania nacional e aquelas condutas que são repulsivas de acordo com a cultura daquele local, em contra partida a internet possui uma dimensão maior, pois não apresenta limites em relação a um Estado, pois a mesma é vista como uma verdadeira "aldeia global".

4 DAS NOÇÕES GERAIS DOS CRIMES CIBERNÉTICOS

Como já destacado em tópico anterior, o debate referentes os crimes na internet se mostra relevante, tendo em vista que a constante evolução tecnológica, em especial da internet e dos meios de comunicação e informação virtual, mudando, assim, a vida do homem moderno. A consequência dessa modernização também sofre interferência no Direito, em especial no campo do Direito Penal.

Diante disso, na medida em que a internet armazena, processa e transfere uma grande quantidade de informações e dados, acaba por tornar esse espaço virtual propenso á prática de crimes ou de condutas que ferem os bens relevantes para o Direito. Por isso, Auriney Uchôa de Brito registrou a influência da informática para as práticas de delitos virtuais, conforme transcrito a baixo:

Alguns fatores como a intensificação dos relacionamentos via internet, a produção em série de computadores, a popularização do comércio eletrônico (*e-commerce*) e o aumento de transações bancárias, estão diretamente ligados ao aumento de ocorrências de crimes conhecidos, mas que praticadas pela internet ao surgimento de novos valores e logicamente às novas condutas delitivas. (BRITO, 2009)

Por isso, que se tornou um fato relevante para estudo do Direito a inserção da temática referente aos crimes virtuais no estudo do Direito Penal, pois essas condutas que ferem a paz do ordenamento jurídico interno, independente de se apresentar em uma plataforma virtual, devem ser tuteladas pelos operadores do Direito, assim como conceitua o doutrinador Rogério Greco:

Na verdade, sob essa denominação se abrigam não somente os crimes em que o objeto material da conduta praticada pelo agente é um componente informático, a exemplo dos programas de computador ou as próprias informações existentes em um dispositivo informático, como também, e o que é mais comum, todas as demais infrações penais em que a informática é utilizada como verdadeiro instrumento para sua prática. (GRECO, 2013)

Após já analisado acerca da conceituação referente aos crimes virtuais, passamos a analisar os tipos de crimes virtuais, ou seja, como esses crimes virtuais podem ser classificados.

4.1 DA CLASSIFICAÇÃO DOS CRIMES VIRTUAIS

Em primeira análise, devemos estabelecer as diferenças entre crimes próprios e impróprios. Os primeiros são aqueles em que o computador é apenas visto como um instrumento pela qual se executa o crime, por exemplo, no recente caso do jogo da Baleia Azul, em que através da internet era proposta uma série de desafios que levava o participante a cometer suicídio, conforme acentua Tulio Viana:

Por fim, nos casos em que um Delito Informático Próprio é praticado como crime-meio para a realização de um crime-fim não informático, este acaba por receber daquele a característica de informático, razão pela qual o denominaremos de Delito Informático Mediato ou Indireto. (VIANA, 2003)

Nesse sentido, os delitos informáticos mediatos ou indiretos que são aqueles conhecidos como delito-fim, quando um crime cibernético é praticado como meio para a prática de outro crime comum, por exemplo, quando o agente que, sem a autorização, invade o sistema do computador de um banco e realiza a transferência de valores para sua conta, ou seja, estará cometendo um crime informático e outro patrimonial (furto); e de acordo com o princípio da consunção, será punido apenas pelo crime-fim. Conforme transcreve Tulio Viana:

Delito Informático Mediato ou Indireto é o delito-fim não informático que herdou esta característica do delito-meio informático realizado para possibilitar a sua consumação.

Se alguém invade um dispositivo informático de um banco e transfere indevidamente dinheiro para sua conta, estará cometendo dois delitos distintos: o de invasão de dispositivo informático e o furto; o primeiro, crime informático, o segundo, patrimonial. (VIANA, 2003)

Enquanto nos crimes impróprios que são aqueles em que o bem jurídico atingido é a inviolabilidade dos dados ou informações automatizados, por exemplo, a interceptação

telefônica, como apresentado no art. 10 da Lei nº 9.296, de 24 de julho de 1996.⁴ Nesse sentido Tulio Viana:

Delitos informáticos Impróprios são aqueles nos quais o computador é usado como instrumento para a execução do crime, mas não há ofensa ao bem jurídico inviolabilidade da informação automatizada (dados). Sua popularidade é grande e, na maioria das vezes, para seu cometimento não há necessidade que o agente detenha grandes conhecimentos técnicos do uso de computadores. Hipótese clássica de crimes informáticos impróprios são os delitos contra a honra cometidos pelo simples envio de um e-mail (VIANA, 2003).

Outra forma de classificação se trata dos delitos informáticos mistos que são aqueles crimes complexos em que são violados tanto dados informáticos quanto outro bem jurídico tal como nos Art. 67, VII, da Lei nº 9.100/95⁵. Nesse sentido, o doutrinador Teixeira entende essa classificação como:

Crime de informática misto se consubstancia nas ações em que o agente visa o bem juridicamente protegido diverso da informática, porém o sistema de informática é ferramenta imprescindível. (Teixeira, 2014)

Assim sendo, os crimes virtuais podem ser classificados nas mais diversas formas, tendo apenas como conexão a situação está interligada ao meio de tecnologia e suas diversas páginas de interação.

4.2 DAS PRINCIPAIS PRÁTICAS CRIMINOSAS EM AMBIENTE VIRTUAL

Na plataforma digital pode ser propensa a prática de diversos crimes, porém no presente trabalho iremos citar aqueles que possuem um maior destaque na sociedade, pois existe uma lista extensa e com a universalização da internet sua prática aumentou consideravelmente. Em primeira análise podemos observar a prática do crime de pornografia na internet e pornografia infantil, pois com o desenvolvimento da tecnologia houve uma facilidade para a disseminação de matérias multimídias, inclusive de teor pornográfico.

Tendo Gustavo Testa Corrêa⁶ realizado uma classificação para esse tipo de indústria. A primeira classificação é aquela que diz respeito a um grupo que procurava conteúdo erótico que somente tinha acesso àquelas pessoas que são maiores de idade. Enquanto a segunda

⁴ Art. 10 da Lei nº 9.296, de 24 de julho de 1996, que enuncia: “constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei. Pena: reclusão, de dois a quatro anos, e multa.” (BRASIL, 1996).

⁵ Art. 67, VII, da Lei nº 9.100, de 29 de setembro de 1995, que constitui como crime eleitoral a conduta de obtenção indevida do acesso ao sistema de dados eleitorais com o fim de alterar a computação de votos, punindo também a tentativa (BRASIL, 1995).

⁶Gustavo Testa Corrêa, Aspectos jurídicos da Internet, p. 45-46.

classificação era composta por empresas que se utilizavam desse meio para comercialização por meio da Internet. Já terceira classificação é aquela referente ao compartilhamento de conteúdo sobre pedofilia ou de material obsceno, levando uma preocupação para os operadores é que esses praticantes agem de maneira discreta, o que acaba por dificultar o conhecimento de seus autores (Corrêa, 2010).

No que diz respeito à pornografia infantil, esta é tratada como uma conduta dolosa tendo em vista de comercializar um material de teor sexual em criança, independente de ter sido comercializado, bastando a simples posse para consumir o delito, conforme já presente no Estatuto da Criança e Adolescente (Lei 8069/90) em seu artigo 240 e 241⁷.

Outro crime que possui grande ênfase no cotidiano é aquele referente às fraudes virtuais, sendo esse delito caracterizado por uma invasão a determinado grupo de computador para posteriormente realizar modificação em dados do sistema, com a finalidade de obter algum tipo de vantagem, por exemplo, quando ocorre adulteração de depósitos bancários, previsto no Art. 154-A do Código Penal.

Porém, existe uma discussão sobre o momento em que iria ser considerado consumado esse delito. Diante disso, Lima afirma que é preciso que um agente pratique o ato da invasão, modificação, supressão ou pagamento de informações, dados eletrônicos ou programas, ou qualquer outro meio que possa possibilitar uma modificação em um sistema de processamento de dados (2005).

Outro crime de bastante respaldo no meio virtual é o Cyberbullying que pode ser conceituado como é um tipo de violência praticada contra alguém por meio da internet ou de outras tecnologias relacionadas, ou seja, essa prática retoma a ideia de usar o meio virtual para humilhar ou hostilizar uma pessoa atacando-a, inclusive de forma anônima. Nesse mesmo sentido, Melo (2011) afirma:

A internet possibilita colocar online as agressões “verbais” sem que seja necessário estar diante da vítima. Essas agressões “verbais” podem ter várias conotações: [...] revidar ofensas não respondidas em tempo real; expressar opiniões constrangedoras e aviltantes sobre outra pessoa; difamar oponentes mais fortes; caluniar, fazer intrigas, fofocas [...]; colocar apelidos depreciativos, fazer gozações, xingar, insultar, aterrorizar, irritar, humilhar ou quaisquer outras formas de agressão psicológica ou moral (MELO, 2011).

⁷ Art. 240 – Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente:

Pena – reclusão de 4 (quatro) a 8 (oito) anos, e multa.

Art. 241 – Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:

Pena – reclusão 4 (quatro) a 8 (oito) anos, e multa.

Esse tipo de conduta delituosa possui sua própria individualidade, bastante diferente do bullying tradicional que consegue facilmente descobrir a autoria delitiva, pois nos crimes virtuais o autor age de forma anônima e poderá ser praticada a qualquer momento e não apenas quando encontrar a vítima. O grande problema desse crime é a quantidade de usuários que recebem os insultos e velocidade com que eles se propagam.

Esse cyberbullying é derivado de outros crimes já devidamente tipificados no Código Penal, sendo os mais comuns os crimes de Injúria, Difamação, Ofensa, Falsa Identidade, Calúnia, Ameaça, Racismo, Constrangimento Ilegal e Incitação ao Suicídio que está cada vez mais comum, principalmente nos meios de comunicação virtual.

Outro crime bastante comum é o crime de pirataria de software tutelado pela a lei 9609/98 que trata da pirataria de dados eletrônicos, protegendo a autoria dos inventores e programadores de software, ocorrendo por meio de “copyright” de um determinado programa, semelhante ao que ocorre com pirataria de outros bens de propriedade intelectual, tendo apenas como diferença que nesse delito não irá necessitar de um intenso suporte material, por exemplo, na utilização de embalagem, ficando na maioria das vezes disponível na própria área virtual por meio de *download* em *sites*, pois por meio da tecnologia P2P (Peer-To-Peer), um usuário da rede pode compartilhar arquivos com outros milhares de usuários ligados no mesmo plano, bem como conceituado por W. Kellerer:

Uma arquitetura de rede distribuída pode ser chamada Peer-to-Peer (P-to-P, P2P,...) se os participantes compartilharem parte de seus próprios recursos de hardware (poder de processamento, capacidade de armazenamento, banda de rede, impressoras,...). Esses recursos são necessários para prover os serviços e conteúdo oferecidos pela rede (ex. compartilhamento de arquivos ou espaços de trabalho para colaboração mútua). Os serviços e recursos são acessíveis por todos os pares sem necessidade de passar por nenhuma entidade intermediária. Os participantes dessa rede são tanto provedores de recursos (serviços e conteúdo) como demandadores. (Kellerer, 1998)

O amplo cenário envolvendo os diversos delitos que podem ocorrer através de um meio tecnológico, mostra a gravidade da situação e que não se deve mais negar e fechar os olhos para essa visão distorcida de como está sendo utilizada a tecnologia.

5 PROBLEMA DE REPRESSÃO

Na primeira apreciação sobre o tema do problema de repressão aos crimes virtuais, não podemos deixar de observar que uma lei é criada nos moldes da sociedade do mesmo, e, tendo em vista que o Código Penal foi constituído em 1940, não se pode esperar que o mesmo

já possuísse uma normatividade sobre os crimes cibernéticos, pois tais delitos são considerados novos na história do Direito.

Porém, essa circunstância não pode ser considerada como uma desculpa para o Estado se omitir sobre como deveria tratar em caso de delitos que se apresentam na esfera virtual, pois tal situação levaria a ferir o princípio da inafastabilidade da jurisdição, algo inadmissível para um bom funcionamento social, pois sua ausência traz um sentimento de injustiça e insegurança jurídica na sociedade.

Diante disso, mesmo com as dificuldades apresentadas sobre a legislação penal vigente encontrar dificuldade sobre qual lei admitida para aquele fato e qual o procedimento que deverá ser adotado, podemos observar no que diz respeito aos crimes cibernéticos impróprios, mistos e indiretos será tratado como crimes comuns, pois violam bens jurídicos já protegidos pelo Estado, tendo, porém que entender que tal entendimento se faz por meio da analogia e essa situação somente será possível para beneficiar o réu. Todavia, o grande problema surge na hora de tutelar o tratamento referente aos crimes cibernéticos próprios, conforme representado por Fiorillo e Conte.

O grande desafio apontado em relação aos crimes informáticos diz respeito, sobretudo, aos ditos crimes informáticos puros, que não possuem respaldo na legislação pátria, tal como aquele em que há violação à informação considerada como bem juridicamente relevante. (Fiorillo e Conte 2016)

Outro problema relevante sobre a aplicação da lei penal nos crimes cibernéticos é que o Direito Penal se rege na interpretação do Princípio da Legalidade, devidamente abraçada pelo o artigo 1º do Código Penal⁸ e pela a Constituição Federal em seu artigo 5º, inciso XXXIX⁹ que afirma que não haverá crime sem lei anterior que defina e pena sem prévia cominação legal, ou seja, o Estado somente aplicará o seu poder de punir quando já existisse uma lei que demonstrasse a criminalização daquela conduta, pois do contrário será considerado um fato atípico.

⁸ Art. 1º - Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal. (Brasil, 1984)

⁹ Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes(Brasil,1988)

XXXIX - não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal;

Nesse mesmo sentido podemos aplicar o artigo 5º, inciso II da Constituição Federal¹⁰ que ninguém será obrigado a fazer ou deixar de fazer algo senão em virtude da lei, garantindo novamente a presença de uma lei anterior que tipifique que aquela conduta fere os princípios gerais da sociedade e somente assim poderá ser exigida pelo Estado, pois visa proteger os indivíduos de condutas arbitrárias por parte do Estado.

Porém, tais situações não devem ser vistas como desculpas para que o Estado deixe de cumprir o seu direito-dever de punir aquelas condutas que atrapalham uma boa condução da paz social, por isso o Direito deve-se adaptar na mesma proporção em que ocorre a mudança na sociedade. Conforme essa síntese pode-se destacar o caso que obteve grande repercussão nacional referente à aprovação da Lei nº 12.737/2012, também nomeada como “Lei Carolina Dieckmann”, sobre o fato de ter ocorrido divulgação de fotos íntimas de uma atriz na internet, que aparentemente teve suas fotos íntimas copiadas de seu computador, além de ter sido extorquida e ameaçada pelos criminosos.

O surgimento dessa lei trouxe um ar de esperança para a sociedade que já se encontrava inconformada com a omissão que o Estado estava tendo quando se deparava com um ilícito penal que ocorria por meio da Internet e das Tecnologias de comunicação, pois essa lei tratava de maneira exclusiva aqueles delitos praticados em sistemas informáticos, passando, assim, a prevenir e a tipificar os crimes cibernéticos próprios ou puros.

Na referida lei em seu artigo 2º, o legislador criou a seguinte norma penal incriminadora: “Invasão de dispositivo informático” que trouxe uma significativa mudança para o Código Penal, pois passou a inserir essa matéria no seu dispositivo legal do artigo 154-A¹¹.

Nos termos do artigo em seu parágrafo primeiro tipifica a prática do mesmo crime aquele que “produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta acima definida”. (Brasil, 1948)

¹⁰ Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (Brasil,1988)

II - ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei;

¹¹ 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”.(Brasil, 1948)

Diante disso o doutrinador Damásio de Jesus faz relevante entendimento sobre como se configura a conduta praticada referente àqueles que se enquadram no tipo legal do artigo 154-A do Código Penal:

A ação descrita no tipo reside em “invadir”, isto é, ingressar ilicitamente, sem autorização expressa ou tácita do titular do Direito.

O objeto material é o dispositivo informático alheio, aqui incluindo meios físicos e eletrônicos. São exemplos dos primeiros: *computadores, notebooks, tabletes, smartphones, pen drive*; podem ser citados, dentre outros arquivos de armazenamento virtual e caixas de e-mails.

A conduta deve ser praticada por meio da violação indevida de mecanismo de segurança (senhas, firewalls ou programas “antivírus”) (Damásio, 2015).

Embora essa lei tenha sido um marco importante para a tipificação dos crimes virtuais no sistema legal brasileiro, a mesma trouxe uma lacuna perigosa para o operador do Direito, pois caso o criminoso cibernético venha a invadir um dispositivo informático, mas não atender as elementares do tipo penal, irá tornar o fato atípico, ou seja, não será crime e trará novamente o sentimento de impunidade.

6 CONSIDERAÇÕES FINAIS

A internet e a tecnologia se transformaram em um marco civil para a humanidade, pois a cada segundo um grande número de usuários estão se conectando e compartilhando um intenso número de informações, constituindo, assim, o grande universo virtual.

Essa dinâmica constante de comunicação entre usuários traz consigo uma propensa tendência na realização de delitos nessa plataforma virtual, pois aqueles que utilizam dessa prática acreditam que não sofreram a sanção do Estado. Porém, essa situação não poderia está mais errônea, pois, assim como no mundo real, o mundo cibernético também se encontra amparado pelo o Direito e sobre sua concepção daquilo que é ou não permitido, pois nesse mesmo meio se faz necessário à imposição de regras para que as pessoas consigam manter uma relação harmoniosa de convívio.

Embora tenha ocorrido a produção da lei 12.965/14, conhecida como Marco Civil da Internet que veio para regulamentar as relações entre os usuários da internet, a mesma lei trouxe uma lacuna a respeito dos crimes realizados no cenário virtual.

Contudo, o cenário atual, vem mostrando cada vez mais que a prática desses atos criminosos vem cada vez mais atingindo um maior número de pessoas e, consecutivamente, vem se tornando uma conduta ilícita cada vez mais comum, por isso se faz necessário à

adoção de tutela do Estado por meio de ferramentas legais para combater esse tipo de conduta de forma condizente e eficaz.

Diante dessa situação, o plano legal carece de uma maior regulamentação, principalmente no que diz respeito a uma lei individualizada desses atos e que o seu funcionamento seja de forma independente, pois do contrário irá ocasionar lacunas, na qual os criminosos aproveitaram dessa situação para efetuar suas ações delituosas. Logo, sem a aplicação de uma lei efetiva irá torna difícil à atuação do Estado no seu poder-dever de punir.

Em síntese, a elaboração de penas mais severas, leis penais mais positivas, melhor fundamentadas e com aplicação devida irá trazer de volta a segurança jurídica buscada no direito penal na sua função social de proteção aos bens jurídicos, pois passaria a possibilitar uma proteção integral e de forma mais eficaz contra os crimes nas plataformas virtuais.

Cabe também analisar que as condutas delituosas praticadas no cenário virtual, por exemplo, no art. 154-A, parágrafo único do Código Penal que disciplina que tal conduta se trata de uma ação penal condicionada à representação, logo, se faz necessário o conhecimento da autoria delitiva para poder realizar o boletim de ocorrência em contrapartida muitos desses delitos acontece de forma anônima, sendo necessária uma intensa investigação criminal até chegar o conhecimento do autor do crime que por muitas vezes só descobre a autoria depois de ter passado o prazo decadencial.

Outra controvérsia nessa mesma questão se refere ao tratamento desses delitos como crimes de menor potencial ofensivo e com cominação de pena em um número inferior, conforme no caso do art. 154-A do Código Penal que tem sua pena máxima a um ano de detenção, logo, no que diz respeito à prescrição desse delito ocorrerá em quatro anos, conforme presente no art.109, V do Código Penal¹². Portanto, para esse delito é prescrito em poucos anos, levando novamente uma dificuldade na sua punição,

Por fim é importante ressaltar que é necessário denunciar os crimes virtuais, pois o próprio judiciário permite no âmbito administrativo fazer uma denúncia através da própria internet, por exemplo, quando o Ministério Público Federal no Estado de São Paulo, oferta em seu site uma ferramenta “Digidenuncia” que ao acessá-la o usuário poderá realizar sua

¹²**Art. 109.** A prescrição, antes de transitar em julgado a sentença final, salvo o disposto no § 1o do art. 110 deste Código, regula-se pelo máximo da pena privativa de liberdade cominada ao crime, verificando-se (Brasil, 1948)

V - em quatro anos, se o máximo da pena é igual a um ano ou, sendo superior, não excede a dois;

denúncia, inclusive de forma anônima. Outra forma que tornaria mais efetivo o combate a esses delitos seria a possibilidade da criação de delegacias especializadas em Crimes Cibernéticos, conforme ocorre em algumas cidades, facilmente encontradas no site do Instituto de Defesa Cibernética.

Com isso os usuários da internet com as suas diversas formas de utilizar a tecnologias podem atuar nessa plataforma de forma adequada ou inadequada. Por isso, se faz necessário estabelecer regras para a atuação no ciberespaço, ou seja, estabelecer como deverá ser uma conduta coerente por parte de seus usuários por meio de normas de como se comportar de forma adequada dentro do universo virtual.

REFERÊNCIAS

- BRITO, Auriney Uchôa de. *O bem jurídico-penal dos delitos informático*, p. 14.
- CORRÊA, Gustavo Testa. *Aspectos Jurídicos na Internet*, 5, ed. Saraiva, 2010
- FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. **Crimes no Meio Ambiente Digital**. 2. ed. São Paulo: Saraiva, 2016.
- FURLANETO NETO, M.; Guimarães, J.. Crimes na Internet : elementos para uma reflexão sobre a ética informacional. **Revista CEJ**, América do Norte, 720 03 2003.
- GRECO, Rogério. Curso de direito penal: Parte especial. 10. ed. Niterói: Impetus, 2013. Vol. II, p. 598.
- INSTITUTO DE DEFESA CIBERNÉTICA. Disponível em: <http://www.idciber-eb.unb.br/>, acesso em 10 de Novembro de 2019.
- JESUS, Damásio. **Direito penal: parte especial 2**. 35, ed. Saraiva, 2015, p.344
- LEI CAROLINA DIEKMANN. Disponível em :<http://g1.globo.com/tecnologia/noticia/2013/04/lei-carolina-dieckmann-que-pune-invasao-de-pcs-passa-valer-amanha.html>, acesso em 5 de Novembro de 2019.
- LIMA, Maria de La Luz apud FURLANETO NETO, Mário; GUIMARÃES, José A. Chaves, op. cit., mar. 2003. P. 70.
- LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional**. Campinas, SP: Ed. Millennium, 2005.
- MARCO CIVL DA INTERNET. Disponível em: <https://super.abril.com.br/mundo-estranho/o-que-e-o-marco-civil-da-internet/>, acesso 10 de Novembro de 2019
- MELO, Josevaldo Araújo de. **Cyberbullying: a violência virtual**. 2ª Edição. Recife:EDUPE, 2011

MINISTÉRIO PÚBLICO: DIGIDENÚNCIA. Disponível em: <https://fernandorodrigues.blogosfera.uol.com.br/2013/05/14/ministerio-publico-abre-canal-para-receber-denuncias-de-crimes-digitais/>, acesso 10 de Novembro de 2019.

PLANTULLO, V. L. Estelionato Eletrônico. Curitiba: Juruá, 2003.
Presidente Prudente: [s.n.], 13/04/2015. Disponível em: <http://www.egov.ufsc.br/portal/conteudo/o-direito-frente-%C3%A0-era-da-inform%C3%A1tica>>. Acesso em: 28/05/2019.

REDIVO, R.; MONTEIRO, G. L. **O DIREITO FRENTE À ERA DA INFORMÁTICA**. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/1411-2489-1-pb.pdf> . Acesso em: 12 de maio de 2019.

REIS, Maria Helena Junqueira, op. cit., 1997. p.25.

ROSA, Fabrício. Crimes de Informática. Campinas: Bookseller, 2002

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

TEIXEIRA, Tarcisio. Curso de direito e processo eletrônico: doutrina, jurisprudência e prática. São Paulo: Saraiva, 2014.

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

W. Kellerer, Dienstarchitekturen in der Telekommunikation -Evolution, Methoden und Vergleich, Technical Report TUM-LKN-TR-9801, 1998.