PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO E RELAÇÕES INTERNACIONAIS
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUTA DE TRABALHO DE CURSO
PROJETO DE TRABALHO DE CURSO I

CIBERCRIMINALIDADE NO BRASIL: APLICAÇÃO, FALIBILIDADE E IMPUNIDADE

ORIENTANDO – GABRIEL FERREIRA QUEIROZ
ORIENTADOR – PROF. DOUTOR GERMANO CAMPOS SILVA

GOIÂNIA
2021

GABRIEL FERREIRA QUEIROZ

CIBERCRIMINALIDADE NO BRASIL: APLICAÇÃO, FALIBILIDADE E IMPUNIDADE

Artigo científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito e Relações Internacionais, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).

Prof. Orientador – Doutor Germano Campos Silva

GOIÂNIA

2021

GABRIEL FERREIRA QUEIROZ

CIBERCRIMINALIDADE NO BRASIL: APLICAÇÃO, FALIBILIDADE E IMPUNIDADE

Data da defesa: 18 de novembro de 2021

BANCA EXAMINADORA

Orientador: Prof. Dr. Germano Campos Silva Nota

Examinador Convidado: Profª. Dra. Rosângela Magalhães Nota

SUMÁRIO

CIBERCRIMINALIDADE NO BRASIL: APLICAÇÃO, FALIBILIDADE E IMPUNIDADE

Gabriel Ferreira Queiroz

RESUMO

O presente artigo tem como objetivo a aplicação do Código Penal Brasileiro nos crimes virtuais, e dentro desse contexto procura responder à problemática sobre a constatação e aplicabilidade nos crimes virtuais e as suas possíveis soluções. Para que esse problema fosse resolvido com maior abrangência possível certas questões de suma relevância devem ser abordadas, a exemplo, o que é e, ou, podem ser considerados crimes virtuais, a definição e estipulação do que seria o espaço virtual e suas peculiaridades, a definição acerca do local de apuração e competência destes crimes nesta modalidade. O estudo tem como foco central mostrar de que maneira as atuais medidas tomadas, se melhor ou devidamente aplicadas de maneira divergente à atual, contida no Direito Penal Brasileiro, puniriam com maior eficácia. No intuito de averiguar como na atualidade é lidado com este problema, suas implicâncias, fatos e problemáticas, as dinâmicas atuais; assim convergindo sobre suas aplicabilidades e confrontando-as com o ordenamento Jurídico brasileiro, e se chegando à conclusão sobre sua respectiva eficiência. Com vislumbre, em caso positivo, para adaptar essas medidas, assim melhorando a eficiência, aplicabilidade e utilização de nosso Direito Penal para estas práticas delitivas.

PALAVRAS CHAVE: Crimes Virtuais, Espaço Virtual, Punibilidade.

INTRODUÇÃO

O computador digital foi criado em 1946, chamado de ENIAC, ele tinha a simples e única finalidade de automatizar o cálculo de tabelas balísticas. E desde lá até hoje muitas mudanças quanto à sua finalidade ocorreram, hoje ele é utilizado de maneira global e com diversas finalidades, seja para realizar cálculos, fazer compras, ou mesmo expressão através da simples comunicação virtual, e ao mesmo tempo o homem incide nele, o meio virtual, e também demonstra um de seus aspectos mais singelos e obscuros, presente desde a antiguidade, a criminalidade.

O meio virtual tem se apresentado como local de grande incidência da criminalidade, de modo que o desconhecimento de alguns tornam-se a poder e lucro para outros. “A internet é uma grande praça pública, o maior espaço coletivo do planeta”. (CASSANTI, 2014, p.3)

Ciberespaço é definido como um mundo virtual pois está em presente potência, hoje em dia a internet é usada no mundo inteiro e ela se encontra em somente um espaço o que o torna desterritorializante. Não há como medi-lo, logo esse mundo também não é palpável, mas existe de outra forma, nos computadores, celulares e equipamentos eletrônicos sendo outra realidade. (MONTEIRO, 2007)

E que se frise, que esse campo sempre foi uma área muito fértil para o crime, e com a globalização até mesmo esse se espalha em grande velocidade e larga escala. São muitos os crimes associados a esse tipo de utilização, alguns mais simples e facilmente perpetrados e outros mais complexos e que requerem amplo conhecimento por parte de quem o comete. Sendo o maior incentivo de quem os comete é a falsa sensação de um ambiente sem leis gerado pelo meio virtual.

Segundo Antônio Chaves, cibernética é a “ciência geral dos sistemas informantes e, em particular, dos sistemas de informação.” (CHAVES, Antônio apud SILVA, Rita de Cássia Lopes. Direito Penal e Sistema Informático, p. 19.) Sendo a ciência da comunicação e dos sistemas de informação, parece o termo mais amplo, e apropriado, a denominação dos delitos tratados nesse trabalho de crimes cibernéticos.

Tratando-se de um lado engano pensar que as trocas de informações seriam seguras, afinal o crime é de natureza humana, que sempre é suscetível à corrupção. O Direito Penal brasileiro encontra muitas dificuldades ao tentar adentrar esse domínio. Pois parece não conseguir se manter lado a lado com os avanços proporcionados pela evolução tecnológica que é a internet. E é nesse domínio, totalmente livre, que se desenvolveu uma nova modalidade de crimes, crimes estes que tem acompanhado esse ritmo e contribuído para o surgimento de novas ameaças, são os chamados crimes virtuais, perpetrados por aqueles que se aproveitam da possibilidade de anonimato e da ausência de regras na rede mundial de computadores.

O presente trabalho tem como ideia fundamental expor na primeira seção as distintas dimensões do espaço virtual, discorrer sobre o espaço virtual enquanto “abstrato” e demonstrar que é um espaço em que as relações têm consequências no “mundo real”. Na segunda seção o objetivo é mostrar o espaço virtual sob a ótica do direito penal, ressaltando a necessidade de um regramento específico no brasil e transparecer a definição, classificação e tipificação dos denominados cibercrimes, além de amostrar que o tempo e o espaço são complicadores na aplicação da lei penal nesses delitos. Já a última seção deste artigo tem como propósito campear através das normas aplicáveis os elementos específicos ao processo criminal dos cibercrimes, demonstrando como agir em casos de crimes virtuais e como funciona a investigação e apuração judicial da autoria e da materialidade do crime para que no fim possa haver a conclusão do tema.

1. AS DISTINTAS DIMENSÕES DO ESPAÇO VIRTUAL

Discorrer ou mesmo conceituar o ciberespaço (ou espaço virtual) não é tarefa fácil, pois como se define um espaço do qual não possui “espaço”, que não ocupa espaço, que não possui representação física, mas que, porém, afeta a vida e condis em resultados no mundo facto. O mesmo, apesar de difícil, já que não existe um consenso, trata-se de um espaço, quase que em sua maioria, reservado à comunicação, mesmo que com local indefinido e impalpável.

A internet pode ser considerada o principal ambiente do ciberespaço (ou espaço virtual), devido à sua popularidade e utilização, mas ele também incorre em outras tecnologias, como serviços de comunicação: celulares, satélites, redes de informação, entre outras.

Gibson (2003) foi o primeiro a se utilizar desse termo referindo-se a este espaço, em 1984, porém terminologicamente sua origem, da palavra Cyber, vem do grego, que significa controlar ou direcionar; logo o significado da palavra ciberespaço é espaço controlado ou espaço dirigido.

Na definição de Gibson:

> Uma alucinação consensual vivida diariamente por bilhões de operadores autorizados, em todas as nações, por crianças aprendendo altos conceitos matemáticos.... Uma representação gráfica de dados abstraídos dos bancos de dados de todos os computadores do sistema humano. Uma complexidade impensável. Linhas de luz abrangendo o não-espaço da mente; nebulosas e constelações infindáveis de dados. Como marés de luzes da cidade. (GIBSON, 2003, p.67)

Conceitua Silvana Drumond Monteiro que:

> Ciberespaço é definido como um mundo virtual porque está em presente potência, é um espaço desterritorializante. Esse mundo não é palpável, mas existe de outra forma, outra realidade. O ciberespaço existe em um local indefinido, desconhecido, cheio de devires e possibilidades. Não podemos, sequer, afirmar que o ciberespaço está presente em nossos computadores, tampouco nas redes, afinal onde fica o ciberespaço? Para onde vai todo esse “mundo” quando desligamos nossos computadores? É esse caráter fluido do ciberespaço que o torna virtual. (MONTEIRO; 2004)

O ciberespaço é um novo local de consulta de dados, possibilitado pelo avanço da tecnologia. Uma nova técnica ou método que absorve a todas as outras e dispõem recursos inimagináveis. Consiste em um espaço novo, que não se tem muito conhecimento, com muitos desafios e incertezas. Um espaço ou local em branco, impalpável, sem existência ficta, um local construído sobre sistemas e totalmente abstrato.

Se por certo aspecto o ciberespaço se entende como do conceito máquina abstrata, e ao realizá-lo encontramos sua dimensão na grande vasta das definições que se encontram na ciência sobre o mesmo, por outro, a denominação máquina abstrata o antecede, lança seu sobrevoo sobre o objeto deste, mas não apenas nele, intencionalmente, conotando-o.

Sendo então o espaço virtual o local de criação de expressões culturais, ou seja, da cultura digital, comercialização, econômica e social, abordaremos o ciberespaço como um espaço semântico/semiótico, desterritorializado, nômade, em fala e escrita devidamente especializada e com aspectos em constante mudança.

O mundo virtual tomou conta da vida das pessoas. As redes sociais mais do que nunca fazem parte da rotina das pessoas, chegando mesmo a trazer problemas de relacionamento, comunicação e administração do tempo.

A população brasileira está cada vez mais conectada. É isso que mostra a Pesquisa Nacional por Amostra de Domicílios (PNAD) de 2019, realizada pelo Instituto Brasileiro de Geografia e Estatística (IBGE). De acordo com o levantamento, 82,7% dos domicílios nacionais possuem acesso à internet, um aumento de 3,6 pontos percentuais em relação a 2018.

É inegável que as redes sociais têm se consolidado como meio de comunicação extremamente dinâmico e eficiente, possibilitando aos seus usuários a propagação de todo e qualquer tipo de informação, em tempo real e âmbito global, de forma gratuita e irrestrita verdadeiramente livre.

No entanto, a liberdade assegurada aos usuários e a eficiência na propagação das informações faz das redes sociais um ambiente propício para a disseminação de ataques pessoais, de informações mentirosas, de discursos de ódio e até mesmo para a prática de crimes, valendo-se o ofensor, na maioria dos casos, do anonimato gerado pela utilização de perfis falsos ou subterfúgios do gênero.

Embora o desenvolvimento de novas tecnologias para a segurança nas redes seja constante, o vazamento de dados na internet ainda é um problema que ocorre frequentemente.

Usuários de todo o mundo fornecem seus dados a todo momento para os mais variados sites e entidades. Seja para cadastros, compras on-line, interação em redes sociais e até transações bancárias.

A violação de dados é configurada como um incidente de segurança, que permite que informações confidenciais abertas sejam analisadas, roubadas, copiadas e usadas por terceiros sem permitir o acesso. O principal motivo do vazamento de informações não são apenas os ataques cibernéticos que muitas pessoas imaginam, mas também as vulnerabilidades de segurança que podem ser facilmente corrigidas. Violar e destruir a confidencialidade de informações confidenciais pode prejudicar pessoas e empresas. Por exemplo, em uma empresa, as violações de dados não afetarão apenas a imagem negativa da organização, mas

também afetarão o andamento de vários processos e transações financeiras. Para os indivíduos, a divulgação de informações pessoais pode levar a tentativas de golpe contra indivíduos. Indivíduos mal-intencionados "roubam sua identidade" para conduzir transações financeiras e cometer crimes em casos extremos.

Como visto até agora, o uso irresponsável da internet traz, além de riscos à segurança das informações, comerciais ou pessoais, vulnerabilidade à honra e imagem do indivíduo. Criou-se margem para a disseminação de discursos de ódio contra grupos minoritários, alvos de preconceito.

Cabe esclarecer que o direito à livre manifestação do pensamento é garantia constitucional, porém a Carta Magna veda o anonimato, isto é, qualquer pessoa tem o direito de expressar suas opiniões desde que se identifique como responsável por elas, para preservar o direito do contraditório. Sob esse aspecto, Pedro Lenza explica que:

> A Constituição assegurou a liberdade de manifestação do pensamento, vedando o anonimato. Caso durante a manifestação do pensamento se cause dano material, moral ou à imagem, assegurasse o direito de resposta, proporcional ao agravo, além da indenização. (LENZA, 2012, p. 981)

Uma afirmação que se pode fazer quando tratando do espaço virtual é que é um espaço em que as relações têm consequências no “mundo real”, e como as pessoas passam diariamente a usufruindo, foi-se mostrado que esse meio virtual pode sim afetar a vida pessoal da pessoa através de crimes virtuais e a cibercriminalidade está presente no dia a dia das pessoas.

Crimes virtuais, até mesmo as próprias legislações criadas em combate aos referidos crimes, é um dos assuntos mais discutidos por juristas, advogados e estudantes hoje no cenário jurídico brasileiro. Assim sendo, as leis representam um grande avanço, em relação a este novo campo de causas danosas, onde que criminosos utilizam deste meio eletrônico, para chantagear, até mesmo extorquir terceiros, com um só proposito subtrair dinheiro, como também fazer com que a vítima faça coisas contra a sua própria vontade.

Para definir o que seja o crime virtual trazem-se conceitos de alguns estudiosos no assunto.

Para Ramalho Terceiro:

> [...] os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo, por isso, ficaram usualmente definidos como sendo crimes virtuais, ou seja, os delitos praticados por meio da internet são denominados de crimes virtuais, devido à ausência física de seus autores e seus asseclas (TERCEIRO, 2009, p.2).

Segundo Augusto Rossini:

> [...] o conceito de “delito informático” poderia ser talhado 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 a confidencialidade (ROSSINI, 2004, p. 110.).

Em outras palavras, crime virtual pode ser aquele que comete qualquer ato típico, antijurídico ou culpável, com objetivo de processamento automático de dados ou sua transmissão em que um computador conectado ou não à rede de computadores mundiais. Portanto, a própria invasão, mesmo não causando danos configura-se crime.

Engana-se, porém, quem pensa que a internet é uma espécie de “terra sem lei”, na qual tais abusos, cometidos por meio das redes sociais, não poderiam ser alcançados e reprimidos pelo Direito. Pelo contrário, existe no Ordenamento Jurídico brasileiro uma série de normas estabelecendo direitos, deveres e mecanismos judiciais aplicáveis no âmbito das redes sociais, insertas no chamado Marco Civil da Internet (Lei 12.965/2014), no Código Civil Brasileiro (Lei 10.406/2002), no Código Penal Brasileiro (Dec-Lei 2.848/40) e na própria Constituição Federal, além de já ter sido o tema objeto de ampla construção literária e jurisprudencial.

2. O ESPAÇO VIRTUAL SOB A ÓTICA DO DIREITO PENAL

De fato, presencia-se o surgimento de novos tipos legais que, dado as suas singularidades, surpreenderam os operadores do direito em geral, em todos os ramos legais, não só em relação à matéria penal. Enquanto não houver uma preocupação por parte dos legisladores, materializando tal ato na formulação de leis que qualifiquem, discriminem e tipifiquem as ações destes agentes como criminosas, os delitos praticados pela internet, serão na sua esmagadora maioria carecedores de uma reprimenda legal.

No presente Código Penal não se encontra nenhum artigo onde enquadre-se o sujeito que comete uma infração por meio de computador. Geralmente punem-se esses criminosos no enquadramento de outros artigos, como estelionato, formação de quadrilha, entre outros.

Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal, preceitos previstos nos incisos II e XXXIX do art. 5º da CF/88, respectivamente, base de todo nosso regime jurídico, sendo assim é inviável o funcionamento atual ser controverso a esse posicionamento, mesmo que algumas decisões já sejam tomadas direcionadas a esse ponto, não é totalmente efetivo o combate a esses delitos.

Em um ambiente virtual, por proporcional é um sentimento de liberdade plena, possibilitando o sigilo (no Brasil é vedado pela CF/88, em seu artigo 5°, inciso IV) e oferecendo um mundo sem fronteiras, possibilitando a prática de crimes complexos, que exigem uma solução rápida e especializada, pois o avanço desses crimes é diretamente proporcional aos avanços da tecnologia e criminosos continuam impunes.

Comportamentos informáticos (com o auxílio de hardware ou software) são ou deveriam ser objeto de legislação penal e não as técnicas ou armas usadas pelo comportamento. Como enunciado, necessita-se sim analisar se as técnicas empregadas estão ou não contidas no comportamento. No Brasil, há mais de 12 anos, busca-se desenfreadamente legislar sobre crimes digitais, de forma errônea

e inconsequente. Os primeiros legisladores buscavam punir técnicas ou armas, como visto, um erro, pois as técnicas, artefatos e as armas cibernéticas se modificam. Posteriormente, passaram a definir dezenas de comportamentos, uns até mesmo que coincidiam com outros, gerando uma redundância criminal. Em um terceiro estágio, onde fora possível a aprovação das Leis de Crimes Informáticos, objeto do presente livro (Leis n. 12.735/2012 e n. 12.737/2012), chegou-se ao acordo de dar relevância penal apenas a comportamentos considerados intoleráveis ou recorrentes na sociedade. Comportamentos (ou condutas) são relacionados a potenciais crimes próprios, onde a informática é o bem jurídico agredido. Logicamente, não se enumera os comportamentos que ofendem outros bens jurídicos, e que podem ser realizados por intermédio da informática, como, por exemplo, encartados nos delitos de pornografia infantil, contrafação, pirataria de software, a ameaça, a injúria, dentre outros. Para estes, o Código Penal é suficientemente claro.

Existem hoje basicamente no ordenamento jurídico brasileiro duas leis que regulamenta os crimes virtuais. A mais antiga é a lei ordinária 12.735/2012 e a lei 12.737/2012, que ficou conhecida nacionalmente como “Lei Carolina Dieckman”, criada após o vazamento de fotos pessoas da atriz do seu computador pessoal.

Apesar de existirem essas duas Leis específicas devemos reconhecer que elas não são suficientes para regulamentar as infrações cometidas. Além da necessidade de serem criados mecanismos específicos e suficientes para punir os infratores.

Percebe-se que a norma jurídica brasileira não acompanhou a evolução dos crimes cibernéticos para coibir os crimes virtuais, o mundo virtual ainda é muito carente de leis específicas para punir tal delito, ou seja, existe um vazio normativo, que permita ao estado punir os infratores.

Projetos de lei já tramitam no congresso, contudo o processo é muito moroso, e devido às grandes mudanças existentes na internet, os meios de regulamentar concretamente se tornam difíceis, tendo isto em mente é que surge a necessidade de uma normatização para o combate efetivo das práticas delituosas efetuadas na rede mundial de computadores, essa situação não deve continuar se

munindo da defasagem da legislação, por isso se faz necessária uma legalização, para combater estas práticas que se firmam cada vez mais em território nacional.

É imprescindível esclarecer que não existe uma única nomenclatura sobre crimes cibernéticos, e sim várias, sendo que não há um consenso sobre a melhor denominação que relacionam os delitos com a tecnologia. Segundo Antônio Chaves, cibernética é a “ciência geral dos sistemas informantes e, em particular, dos sistemas de informação” (CHAVES, Antônio apud SILVA, Rita de Cássia Lopes. Direito Penal e Sistema Informático, p. 19).

Os crimes cibernéticos são praticados das mais diversas formas, é importante ressaltar que os crimes e contravenções penais são compreendidos tanto pelas práticas na internet, quanto pelos sistemas informáticos, pois estes se difundem em ambiente virtual, o qual está repleto de usuários mal-intencionados, que tem por objetivo buscar oportunidades para o cometimento de atos ilícitos.

Existem muitas formas e espécies de cometimento de um crime cibernético, Rodrigo Guimarães Colares nos ensina que:

> Crime contra a segurança nacional, preconceito, discriminação de raça-cor e etnias, pedofilia, crime contra a propriedade industrial, interceptação de comunicações de informática, lavagem de dinheiro e pirataria de software, calúnia, difamação, injúria, ameaça, divulgação de segredo, furto, dano, apropriação indébita, estelionato, violação de direito autoral, escárnio por motivo de religião, favorecimento da prostituição, ato obsceno, incitação ao crime, apologia ao crime ou criminoso, falsa identidade, inserção de dados em sistema de informações, falso testemunho, exercício arbitrário das próprias razões e jogo de azar (2002, p. 02)

Segundo Aloma Ribeiro Felizardo (2010.p.56) os crimes cometidos em ambiente virtual possuem uma lista extensa e com a universalização da Internet, sua prática aumentou notadamente.

Os Crimes virtuais podem ser classificados em próprios ou puros e, ainda, em impróprios ou impuros. Veja-se as seguintes transcrições doutrinárias:

Ações dirigidas contra um sistema de informática, tendo como subespécies atos contra o computador e práticas contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial. (FERREIRA apud CARNEIRO, 2012, [n.p.]).

Didaticamente falando, a classificação mais adequada a atual realidade é a que os crimes podem ser próprios ou impróprios

Os crimes virtuais próprios são aqueles em que o sujeito ativo utiliza o sistema informático do sujeito passivo, no qual o computador como sistema tecnológico é usado como objeto e meio para execução do crime.

Nessa categoria de crimes está, não só a invasão de dados não autorizados, mas toda a interferência em dados informatizados como, por exemplo, invasão de dados armazenados em computador seja no intuito de modificar, alterar, inserir dados falsos, ou seja, que atinjam diretamente o software ou hardware do computador e só podem ser concretizados pelo computador ou contra ele e seus periféricos.

Para certos doutrinadores, como Marco Túlio Viana, crimes virtuais próprios “são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados)” (VIANA, 2003 apud CARNEIRO, 2012).

Corroborando com esse conceito, valiosas são as lições de Damásio Evangelista de Jesus:

> Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado. (DAMÁSIO, 2003 apud CARNEIRO, 2012, [n.p.]).

Os crimes virtuais denominados impróprios são aqueles realizados com a utilização do computador, ou seja, através da máquina que é utilizada como instrumento para realização de condutas ilícitas que atinge todo o bem jurídico já tutelado, crimes, portanto que já tipificados que são realizados agora com a utilização do computador e da rede, utilizando o sistema de informática seus componentes como mais um meio para realização do crime, e se difere quanto a não essencialidade do computador para concretização do ato ilícito que pode se dar de outras formas e não necessariamente pela informática para chegar ao fim desejado como no caso de crimes como: pedofilia.

Do mesmo modo afirma o jurista Damásio E. de Jesus. In *verbis*:

> Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não-computacionais ou diversos da informática. (DAMÁSIO, 2003 apud CARNEIRO, 2012, p. ?)

Essas classificações são eficazes didaticamente para se entender e classificar alguns crimes, mas por conta da rapidez na evolução e dinâmica da rede de computadores e internet fica quase impossível acompanhar e afirmar categoricamente que não há modalidades que não estejam listadas nas classificações adotadas.

Os crimes cibernéticos são classificados pela doutrina brasileira dominante como delito de natureza formal, posto que se consumam no momento da prática da conduta delitiva, independente da ocorrência do resultado naturalístico.

Outrossim, e com muita propriedade acerca desse tema, o jurista Vicente de Paula Rodrigues Maggio (2013, *online*) assim classificou os crimes cibernéticos:

> Trata-se de crime comum (aquele que pode ser praticado por qualquer pessoa), plurissubsistente (costuma se realizar por meio de vários atos), comissivo (decorre de uma atividade positiva do agente: "invadir", "instalar") e, excepcionalmente, comissivo por omissão

> (quando o resultado deveria ser impedido pelos garantes – art. 13, § 2º, do CP), de forma vinculada(somente pode ser cometido pelos meios de execução descritos no tipo penal) ou de forma livre (pode ser cometido por qualquer meio de execução), conforme o caso, formal (se consuma sem a produção do resultado naturalístico, embora ele possa ocorrer), instantâneo (a consumação não se prolonga no tempo), monossubjetivo (pode ser praticado por um único agente), simples (atinge um único bem jurídico, a inviolabilidade da intimidade e da vida privada da vítima).

Quando se levanta a questão da tipificação dos crimes virtuais no ordenamento jurídico brasileiro, logo pensa-se em precariedade, mas muitos não sabem que a legislação brasileira alcança de 90 a 95% os crimes praticados no âmbito virtual em nosso país, pois os crimes praticados por meio do computador para a realização do delito mais conhecido como a modalidade de crimes próprios são normalmente já tipificados em nosso Código Penal.

TIPO PENAL – DISPOSITIVO LEGAL APLICÁVEL

TIPO PENAL	DISPOSITIVO LEGAL APLICÁVEL
Calúnia	Art. 138 do Código Penal
Difamação	Art.139 do Código Penal
Injúria	Art. 140 do Código Penal
Ameaça	Art.147 do Código Penal
Furto	Art.155 do Código Penal
Apropriação Indébita	Art.163 do Código Penal
Estelionato	Art.171 do Código Penal
Violação ao Direito Autoral	Art.184 do Código Penal
Pedofilia	Art.247 da Lei 8.069/90 (Estatuto da Criança e do Adolescente)
Crime Contra a Propriedade Industrial	Art.183 e segs. Da Lei 9.279/96
Interceptação de Comunicação de Informática	Art. 10 da Lei 9.296/96

Interceptação de E-mail Comercial ou Pessoal	Art.10 da Lei 9.296/969
Crimes Contra Software (Pirataria)	Art.12 da Lei 9.609/98

Esses crimes em sua maioria são cometidos por meio da Internet, mas também por meio normal, portanto a previsão legal em sua maioria não o trata como crime virtual e sim como crime penal independentemente do meio utilizado para a sua consumação se for realizado será enquadrado na lei penal em questão.

No âmbito do Direito Penal é de devida importância a apuração de forma sucinta sobre a jurisdição e a competência para a aplicação da lei. Ocorre que os crimes virtuais como visto abrangem todo um território virtual, ou seja, não mensurável, e, isto posto não passível de delimitações físicas, assim interagindo com diversos países.

Quando se pensa na possibilidade de o usuário da rede de internet poder vir a acessar um computador brasileiro através de um IP estrangeiro, assim causando um problema e ao mesmo tempo uma dúvida, o local do crime e a inexatidão quanto à identidade do criminoso.

Não de se deve mensurar o espaço cibernético, visto que é certo que cada país possui sua própria soberania e jurisdição.

Conforme o princípio da territorialidade, utilizado no Brasil, adotamos a teoria da ubiquidade, devidamente prevista e aceita pelo Código Penal Brasileiro, da qual se considera o local do crime tanto o da conduta quanto o do resultado. No Brasil temos a possibilidade de aplicação segundo o artigo 5º de nosso Código Penal, por extensão e sem prejuízo a convenções, regras e tratados internacionais, quando cometido o crime em território nacional.

Diz-se que a impunidade que existe na rede mundial de computadores se deve à falta de uma regulamentação específica na área penal, facilitando, e até estimulando a atuação dos indivíduos desprovidos de maiores escrúpulos.

O Direito é a única forma de controle que pode conter o avanço da criminalidade no mundo virtual, de todos os sistemas de controle social, também é o único que exerce coercitividade, sancionando e punindo as condutas havidas por ilícitas. Apenas lei detém caráter imperativo.

As questões que englobam a rede mundial de computadores e os crimes que são cometidos por meios virtuais tem se tornado um dos maiores desafios da sociedade moderna.

Ponto que merece destaque é a ausência de fronteiras nas relações na rede mundial, não existem limites, não existem imposições, existindo assim uma relevante sensação de impotência do poder público para resolver certas questões que acabam entrando até no âmbito da extradição e territorialidade.

No entanto antes de se legislar é necessário um estudo aprofundado sobre as tendências e evoluções da rede mundial de computadores, seus crimes e mudanças presumíveis, para que assim não se criem leis sem fundamentos significativos, leis estas que podem cair em contradição, virando normas não eficazes, todo cuidado é necessário.

3. ELEMENTOS ESPECÍFICOS AO PROCESSO CRIMINAL DOS CIBERCRIMES

As leis de crimes informáticos (leis 12.735/12 e 12.737/12) entraram em vigor na data de 02 de abril de 2013, elas alteram o Código Penal para tratar dos crimes cibernéticos.

O projeto que na Lei 12.735/2012 tramitou no Congresso Nacional desde 1999 (PL 84/99, na câmara). Em seu texto original era bem extenso e bastante polêmico no sentido da responsabilidade dos provedores de internet, mas apesar disso, durante sua tramitação foi reduzido a quatro artigos e, posteriormente, ficou com artigos em decorrência do veto na sanção, pela então presidente Dilma Rousseff.

Portanto, o referido dispositivo legal traz apenas duas mudanças, a saber: “a primeira” determina a criação em cada estado de setores especializados no combate às ações delituosas em rede de computadores, dispositivos de comunicação ou sistemas informatizados, conforme estipula o artigo 4º. A segunda mudança é em relação ao inciso II do § 3º do art. 20 da Lei nº 7.716, de 5 de janeiro de 1989 presente em seu artigo 5º, que o altera em relação ao racismo, ele autoriza que Juízes determinem a interrupção de conteúdos racistas em qualquer meio de comunicação, tendo como punição uma pena que vai de dois a cinco anos de prisão e multa, conforme estipula seu texto de lei:

> 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 (...);
>
> § 3o (...);
>
> II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio.

Conforme o texto, no Art. 4º Os órgãos da polícia judiciária estruturarão, setores e equipes especializadas no combate às ações delituosas em rede de computadores, dispositivos de comunicação ou sistema informatizado.

Ou seja, as polícias civis de todo o Brasil têm de se adaptar à nova realidade, coisa que não vem ocorrendo, afinal no Brasil as forças policiais não são estruturadas e treinadas para lidar eficientemente com esses tipos de situações, mas o que vem ocorrendo é o contrário, em alguns Estados esse serviço vem se extinguindo.

Em junho de 2013 a Policia Civil do Rio Grande do Norte extinguiu seu núcleo de investigação de crimes de alta tecnologia, núcleo que investigava as os Crimes virtuais no Estado, a portaria normativa que pôs fim foi assinada pelo delegado geral daquele estado, nela ele admite que esse núcleo carece de organização estrutural, pessoal e disciplina de gestão administrativa permanente para se chegar à devida prestação dos serviços públicos. (CASSANTI, 2014)

Já a lei 12.737/12, apelidada como Lei Carolina Dieckmann, torna crime as condutas cometidas através da internet, tais como: invasão de computadores, roubo e/ou furto de senhas, derrubada de sites etc.

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
>
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
>
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
>
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
>
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
>
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
>
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
>
> I - Presidente da República, governadores e prefeitos;
>
> II - Presidente do Supremo Tribunal Federal;
>
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
>
> IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Percebe-se pelo texto da lei que as punições previstas são muito brandas, pois aqui no Brasil a pena de até quatro anos de reclusão, nos casos de crimes sem violência, se modifica em restrição de direitos, então como se percebe não haverá perda de liberdade, apenas restrição de direitos, já que a nova lei apenas prevê um ano de detenção.

As principais modificações que esta nova lei traz são:

a) A interrupção dos serviços de utilidade pública em mídias na internet se torna crime;

b) Os tradicionais cartões de crédito passam a se tornar documento particular, e assim as condutas como roubo, furto, adulteração ou falsificação são regidas por lei já existente;

c) A invasão de dispositivo com objetivo de se obter informações privadas ou com a intenção de se utilizar de forma ilícita passa a ser crime.

d) O desenvolvimento e a distribuição de softwares de grampo, escutas ou controles remotos, desde que para fins ilícitos, passam a ser crime.

Além destes existe o Decreto Federal nº 7.962/13, que entrou em vigor na data de 14 de maio de 2013, seu objetivo era preencher as lacunas no Código de Defesa do Consumidor acerca do comércio em lojas virtuais, ou como é chamado o comércio eletrônico, visto que inexiste legislação específica sobre o processo de compra e venda na internet.

> Com as novas regras, as empresas que atuam no comercio eletrônico terão que dispor em suas páginas informações sobre produtos, fornecedores, serviços e aperfeiçoamento do atendimento ao consumidor. (CASSANTI, 2014, p.94)

Os cibercrimes são punidos de natureza igual ao que se pune qualquer outro crime, sendo imprescindível que as provas estejam devidamente preservadas.

Para se coletar e preservar as evidências em meio eletrônico deve-se imprimir, salvar arquivos em meio eletrônico, e-mails, print screen de telas, ou mesmo a impressão da página pelo escrivão policial (visto que seus atos possuem fé pública), de tudo que possa servir como evidencia e possa desaparecer de maneira rápida e sem deixar vestígios. E sempre se lembrar de que todas as provas são importantes para a investigação.

As provas devem ser armazenadas e protegidas em algum tipo de mídia que seja protegida contra alterações, como CD-R, por exemplo.

Logo após deve-se procurar um cartório e registrar uma ata notarial das evidências, assim atribuindo validade jurídica às provas atribuídas.

> A ata notarial serve para pré-constituir prova dos fatos. Muitas vezes não temos como provar uma situação potencialmente perigosa ou danosa. O tabelião é, portanto, uma testemunha oficial cujo ato vai desencadear a fé pública e fazer prova plena perante qualquer juiz ou tribunal. (CASSANTI, 2014, p.57)

A ata notarial pode ser utilizada para comprovar inúmeros fatos, conteúdos divulgados em páginas da internet, de mensagens e o IP emissor, textos que contenham injuria, calunia e, ou difamação, violação de direitos autorais e de imagem, entre outros.

> Nas verificações (tanto no meio físico, quanto no eletrônico), o tabelião constata os fatos, relatando fielmente tudo aquilo que presenciou. A ata notarial tem força certificante para comprovar a integridade e a veracidade destes documentos, atribuir autenticidade, fixar a data, hora e existência de arquivo eletrônico. (CASSANTI, 2014, p.57)

Após este, deve-se procurar uma delegacia, ou uma das delegacias especializadas em crimes virtuais, e fazer o registro.

Os crimes mais comuns são aqueles contra o patrimônio, como: clonagem de cartões, estelionato e desvio de dinheiro. São os mais investigados pelas diversas delegacias especializadas em crimes virtuais do país. Já os crimes como calúnia, injúria e difamação, os chamados crimes contra a honra aparecem logo em seguida. (CASSANTI, 2014)

No plano normativo, o artigo 1º da Lei de Organização da Investigação criminal define a Investigação criminal como:

> Conjunto de diligências que, nos termos da lei processual penal, se destinam a averiguar a existência de um crime, determinar os seus agentes e a sua responsabilidade, descobrir e recolher as provas, no âmbito do processo.

Neste sentido, está perante uma atividade desempenhada pelos órgãos da Polícia Judiciária e pelos Ministérios Públicos e que faz parte de um sistema normativo que define, molda e condiciona o objeto, os objetivos e os limites da sua atuação

Segundo Gilberto Porto, Criminalística pode ser conceituada como:

> Um sistema que se dedica à aplicação de faculdades de observação e de conhecimento científico que nos levem a descobrir, defender, e interpretar os indícios de um delito, de molde a sermos conduzidos à descoberta do criminoso, possibilitando à Justiça a aplicação da justa pena.(PORTO, apud OPILHAR, ANO E PÁGINA)

Nos crimes cibernéticos, o trabalho pericial é de extrema importância para demonstrar materialidade e autoria do crime. Via de regra, a perícia é realizada na fase policial, até porque muitas delas necessitam serem feitas imediatamente ou logo após a prática do crime.

Além da constante atualização dos peritos criminais, também é necessária constante atualização dos operadores do direito, para que possam atuar de forma mais eficaz. Implantar eventos relacionais ao tema em faculdades de Direito torna-se fundamental na busca de profissionais competentes. Os meios acadêmicos, o próprio Poder Judiciário, e as entidades de classe também devem ser alvo desta capacitação técnica.

Ademais da capacitação jurídica, de suma importância, os operadores do direito devem se adequar à nova realidade mundial, que busca diminuir fronteiras e a celeridade. O conhecimento acerca do ordenamento legal tem que ser associado ao conhecimento sobre as ferramentas virtuais, possibilitando o surgimento de profissionais capazes de solucionar conflitos atuais, que em sua maioria envolvem questões tecnológicas.

O primeiro problema a ser enfrentado nos crimes cibernéticos é a determinação da autoria. Muito dificilmente a pessoa que pretende cometer uma infração penal utiliza sua identificação pessoal real. Há casos em que o criminoso se faz passar por outra pessoa, mediante o uso indevido de suas senhas pessoais.

Nas redes de computadores, não é possível identificar o usuário visualmente ou através de documentos, mas é possível identificar o endereço da máquina que envia as informações à rede. Ou seja, o IP da máquina.

O número IP é uma identificação que todos os computadores que acessam a Internet possuem; ele aparece no formato A. B. C. D, onde A, B, C e D são números que variam de 0 a 255 (por exemplo, 222.177.8.25).

Por isso a importância da cooperação dos provedores de acesso nesse tipo de investigação. Como visto anteriormente, o provedor é o computador que providencia acesso à rede e é responsável por fornecer aos clientes um número de IP para que este se conecte. Portanto, após se conseguir o número de IP utilizado na realização de uma conduta criminosa, é necessário requisitar ao provedor de acesso informações sobre o usuário daquele IP.

Entretanto, a maioria dos serviços de conexão adota o sistema de IP dinâmico. Isso quer dizer que cada vez que uma máquina se conecta a Internet, recebe um IP diferente de seu provedor. Por isso, além de possuir o número de IP utilizado para a prática criminosa, também são necessários a data, a hora exata da conexão ou comunicação e o fuso horário do sistema.

Como a Internet é uma rede mundial de computadores, os registros indicam a hora local e a referência à hora GMT. Às vezes, é feita apenas a menção à hora GMT (por exemplo, “Mon, 07 Oct 2007 00:54:25 GMT”).

Cada IP está vinculado à uma provedora de acesso. Há sites de registro destinados a identificar a provedora de acesso responsável por cada IP. Uma vez identificada a provedora de acesso deve-se requisitar informações a respeito do cliente que utilizou aquele IP durante aquele momento.

“Nos pedidos feitos aos provedores de acesso e às companhias telefônicas, é imprescindível que haja, no mínimo, a menção a esses três indicadores: a) o número IP; b) a data da comunicação; e c) o horário indicando o fuso horário utilizado – GMT ou UTC. Sem eles, não será possível fazer a quebra do sigilo de dados telemáticos. ” (MINISTÉRIO PÚBLICO FEDERAL. 2006, p. 15.)

Importante ressaltar que não se deve confundir “interceptação de dados telemáticos” com “quebra de sigilo dos dados de conexão e de usuário”.

A quebra do sigilo dos dados de conexão de usuário, trata-se somente da disponibilização por parte das empresas, em um primeiro momento, de qual teria sido o IP utilizado e o horário (incluindo informações de fuso horário) de determinada ação criminosa realizada em um serviço de Internet, como redes sociais, contas de e-mail, programas de mensagens instantâneas, dentre outros e em um segundo momento das informações do usuário que efetivamente utilizou aquele IP de

determinado provedor, ou seja, qual teria sido, supostamente, o endereço físico no “mundo real” em que o computador ou outro equipamento informático com acesso à Internet estaria instalado no momento da conduta criminosa.

Já a interceptação de dados telemáticos diz respeito ao recebimento por parte da Autoridade Policial de todos os acessos e conexões realizados pelo investigado em ambiente de Internet. Se equipara, em todas as questões legais, à interceptação telefônica, devendo, portanto, ser realizada em sede de Inquérito Policial, sendo necessária, por conseguinte, a provocação do Poder Judiciário e Ministério Público, por meio de Representação, a fim de obtermos a autorização judicial, nos moldes da legislação vigente, em especial a Lei nº 9.296, a Lei de Interceptações Telefônicas.

Gabriel Cesar Zaccarias de Inelas em sua 2ª edição de Crimes na internet diz que “A análise dos dados constantes dos cadastros de clientes dos provedores de acesso não caracteriza interceptação do fluxo de comunicações em sistemas de informática, sendo certo que a requisição judicial não é necessária.”(INELAS,2009,p.25)

Algumas empresas que prestam serviços na Internet somente divulgam os dados de conexão com decisão judicial. “Costumam criar embaraços para informar à Autoridade Policial as informações que são necessárias à investigação de crimes que tenham sido cometidos em seus serviços”(CORRÊA, online).

Outro problema é o tempo de armazenamento dos logs (anotação das atividades ocorridas no computador ou entre dois computadores) de acesso. Não há na legislação nenhuma previsão de por quanto tempo os servidores devem armazenar essas informações.

Em julho de 2008, o Ministério Público Federal conseguiu com que a Google assinasse Termo de Ajustamento de Conduta, que entrou em vigor imediatamente, prevendo a preservação de todos os dados necessários às investigações pelo prazo mínimo de seis meses e o fornecimento desses dados a polícia brasileira, mediante autorização judicial. Tal acordo foi procedido por inúmeros nos mesmos moldes. Entretanto, tal prazo ainda é incompatível com a conclusão das perícias informáticas e andamento dos inquéritos policiais, sendo a investigação obstaculizada pela perda dessas informações.

Ainda assim, a situação pode ser ainda mais complicada. Marco Aurélio Greco aduz:

> Como identificar o agente? Para termos uma ideia das dificuldades e da complexidade que o tema dos controles assume, por exemplo, na Internet, basta mencionar que podem existir serviços que poderiam ser denominados de 'serviço de máscara. (GRECO, apud INELAS, 2009, p. 117.)

Esses serviços de máscara seriam os denominados proxys (servidor intermediário, que atende a requisições repassando os dados do cliente à frente, a outro servidor, que oferece o serviço) de anonimato. São servidores destinados a promover o anonimato a seus clientes. Muitas vezes, é utilizada uma cadeia de proxys, tornando a identificação da máquina de origem das ações virtualmente irrastreável.

De modo geral, pode-se dizer que as evidências dos crimes cibernéticos são extremamente voláteis. Podem ser apagadas em segundos ou perdidas facilmente. Além disso, possuem formato complexo e costumam estar misturadas a uma grande quantidade de dados legítimos, demandando uma análise apurada pelos técnicos e peritos que participam da persecução penal.

Muitas vezes, para a devida comprovação da materialidade do delito se faz necessária a interceptação do fluxo de comunicações realizadas através de um computador. Tais interceptações, como exposto acima, somente podem ser feitas mediante autorização judicial.

Em relação à inviolabilidade do sigilo das comunicações, Ada Pellegrini Grinover ensina:

> A garantia constitucional pode sofrer limitações, não devendo prestar-se para a proteção de atividade ilícitas ou criminosas. É assim que através de uma ponderada apreciação judiciária, que obedeça aos limites legais, pode ser determinada a interceptação das comunicações telefônicas. (GRINOVER, apud INELAS, 2009, p. 138.)

Observe-se que de acordo com o Parágrafo único do Artigo 1º da Lei nº 9.296 de 24 de julho de 1996, estendeu-se a normatização das interceptações telefônicas às informáticas e telemáticas. Segundo João Roberto Parizatto:

> [...] o que o dispositivo em apreço quer, é estender a aplicação das hipóteses de interceptação de comunicações telefônicas, a qualquer

> espécie de comunicação, ainda que realizada através de sistemas de informática, existentes ou que venham a ser criados. ” (PARIZATTO,ANO p. 18).

A maioria dos crimes cibernéticos exige perícia para sua perfeita prova. Uma vez identificado o endereço real do criminoso, e determinada a busca e a preensão de seu computador e quaisquer mídias que possam conter indícios da materialidade será procedido o exame de corpo de delito.

Inicialmente, é feita uma duplicação das mídias do exame, e a perícia deverá ser realizada nas cópias. Isso porque, além da preservação dos originais, o simples fato de se abrir um arquivo de computador altera seu estado.

Segundo Costa, as “evidências dos crimes cibernéticos, em um computador, podem ser classificadas como evidências do usuário e evidências do sistema”. (COSTA, p. 26.) As evidências do usuário são aquelas produzidas pelo próprio sujeito ativo, em arquivos de texto, imagem ou qualquer outro tipo. Já as evidências do sistema são as produzidas pelo sistema operacional, em função da ação do sujeito ativo. Pode-se citar os arquivos temporários da Internet, o cache da memória (dispositivo de acesso rápido, interno a um sistema, que serve de intermediário entre um operador de um processo e o dispositivo de armazenamento ao qual esse operador acessa) ou os cookies dos sites visitados (grupo de dados trocados entre o navegador e o servidor de páginas, colocado num arquivo de texto criado no computador do utilizador).

CONCLUSÃO

De acordo com a pesquisa, foi visto que é facilmente constatada a dificuldade de se definir o espaço virtual. Devido a isso, torna-se difícil a definição dos cibercrimes para avaliação, demonstrando-se uma tarefa cansativa e árdua, afinal a complicada limitação de seu território, a propensão do anonimato, a falta de conhecimento e treinamento por parte das autoridades investigativas, a grande quantidade de pessoas com a capacidade de conseguir passar técnicas para estes usos tornam a prática de crimes virtuais muito fácil e ao mesmo tempo difícil de se chegar ao responsável e se punir.

E após o estudo acerca do tema, conclui-se que se faz necessário a imediata tipificação em nosso ordenamento jurídico, de condutas criminosas por meio da internet, visto que para combater os crimes em ambiente virtual é aplicada somente o Código Penal e quase sempre os agentes que cometem esse tipo de crime ficam impunes.

No Brasil, ainda não existe uma legislação específica sobre o assunto. Dessa maneira, o tema está atrasado no aspecto jurídico, mas em progresso na criminalidade por meios virtuais. Apesar de existirem iniciativa de projetos de leis, que tem como objetivo regulamentar as condutas delitivas. Dessarte, é indispensável à regulamentação desses crimes virtuais para que prática delitiva não continue empune, assim causando danos à sociedade.

Deve-se lembrar que o Direito deve acompanhar as transformações e mudanças da sociedade, se adaptando à vista disso a sociedade da informação e ao mundo virtual, trabalhando em prol da segurança e garantindo a tutela jurídica dos direitos fundamentais da pessoa humana.

Em um mercado de futuros e que vem crescendo, estamos entre os dez países que mais navegam na internet, sem uma legislação que defina e ordene quantos e quais são os crimes cometidos em ambiente virtual, para proteger os usuários desse serviço.

Os criminosos se aproveitam da necessidade que se tem de usar a internet no cotidiano e de pessoas que não tem conhecimento sobre as possíveis condutas danosas por meio tanto de internet como de telefone, ou seja, por intermédio de algum âmago tecnológico. Porém, infelizmente não temos uma legislação especifica para punir esses malfeitores virtuais.

Em síntese, para que se houvesse eficiência no combate a crimes virtuais seria necessário tratar-se do tema com respeito quanto à criação de leis penais mais efetivas nesse aspecto, no sentido da celeridade e funcionalidade; o asseveramento de suas penas para, por consequência, evitar a sua modificação em restrição de direitos, assim acabando com o clima de impunidade e realçando uma das funções primordiais do Direito Penal que é a de prevenir e por fim melhorar as condições e investir em estruturas, salários, capacitação e fiscalizar os mesmo nos núcleos de combate aos crimes virtuais em cada estado.

Cogita-se a uma maior intervenção do estado na parte de segurança e ética no vasto campo da internet, conforme relata Rosa (2007, p. 43)

Contudo, revela-se necessário também, que para se proteger de ameaças no meio da internet, que os usuários, contem com recursos de segurança, que sejam atualizados de forma constante para prevenção/precaução e detecção de vírus.

REFERÊNCIAS

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. O problema na tipificação penal dos crimes virtuais. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 7, n. 58, 1 ago. 2002. Disponível em: https://jus.com.br/artigos/3186. Acesso em: 25 out. 2021.

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

GIBSON, Willian. Neuromancer. São Paulo: Aleph, 2003.

MONTEIRO, Silvana Drumond. O ciberespaço: o termo, a definição e o conceito. DataGramaZero, Paraná, v.8, n.3. 2007. Disponível em: < http://www.dgz.org.br/jun07/Art_03.htm>. Acesso em 28 de Abril de 2021.

LENZA, Pedro. Direito Constitucional Esquematizado. 16ª ed. São Paulo: Saraiva, 2012.

CASSANTI, Moisés de Oliveira. Crimes virtuais, vitimais reais. Rio de Janeiro: BRASPORT, 2014.

CHAVES, Antônio apud SILVA, Rita de Cássia Lopes. Direito Penal e Sistema Informático. Disponível em: http://schmidtadvogados.com/v/artigo5. Acessado em: 02/06/2021.

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

COLARES, Rodrigo Guimarães. Cybercrimes: os crimes na era da informática <https://jus.com.br/artigos/3271/cybercrimes-os-crimes-na-era-da-informatica> . Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 7 Acesso em: 13 abril 2018.

CARNEIRO, Adeneele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. Âmbito Jurídico, Rio Grande, XV, n.99, abr. 2012. Disponível em: Acesso em: 28 jun. 2021

BRASIL. Lei nº 49 de 27 de Agosto de 2008.

PORTO, Gilberto apud OPILHAR, Maria Carolina Milani. Criminalística e Investigação Criminal

MINISTÉRIO PÚBLICO FEDERAL. Crimes Cibernéticos. Manual Prático de Investigação. 2006, p. 15.

INELAS, Gabriel Cesar Zaccarias de. Crimes na Internet. 2ª edição, 2009, p. 25.

CORRÊA, Rafael. Quebra de sigilo de IP necessita de autorização judicial? Disponível em http://www.rafaelcorrea.com.br/quebra-ip

GRECO, Marco Aurelio apud INELAS, Gabriel Cesar Zaccarias de. Crimes na Internet. 2ª edição, 2009, p. 117.

GRINOVER, Ada Pellegrini apud INELAS, Gabriel Cesar Zaccarias de. Crimes na Internet. 2ª edição, 2009, p. 138.

PARIZATTO, João Roberto apud Idem. Ibidem, p. 138.

COSTA, Marcelo Antonio Sampaio Lemos. Computação Forense, p. 26.

ROSA, Fabrízio. CRIMES DE INFORMÁTICA. 3. ed. Franca: Bookseller, 2007.

MAGGIO, Vicente de Paula Rodrigues. Novo crime: invasão de dispositivo informático - CP, Art. 154-A. 6 p. [internet], 22 out. 2019. Disponível em: https://vicentemaggio.jusbrasil.com.br/artigos/121942478/novo-crime-invasao-de-dispositivo-informatico-cp-art-154-a. Acesso em: 22 out. 2019.

PORTO, Gilberto apud OPILHAR, Maria Carolina Milani. Criminalística e Investigação Criminal

João Roberto PARIZATTO, Comentários à Lei no 9296, de 24.07.96 - Interceptação de comunicações telefônicas, p. 18.