UNIVERSIDADE TIRADENTES – UNIT
CURSO DE GRADUAÇÃO EM DIREITO
TRABALHO DE CONCLUSÃO DE CURSO
ARTIGO CIENTÍFICO

CRIMES VIRTUAIS: APLICAÇÃO, FALIBILIDADE E IMPUNIDADE

Aluno: Aldo Maxwell Pereira de Mesquita Caetano
Orientador (a): Prof.: Jorge Raimundo Valença Teles de Menezes

Aracaju
2015

ALDO MAXWELL PEREIRA DE MESQUITA CAETANO

CRIMES VIRTUAIS: APLICAÇÃO, FALIBILIDADE E IMPUNIDADE

Trabalho De Conclusão De Curso – Artigo Científico – Apresentado Ao Curso de Direito da Universidade Tiradentes – UNIT, como requisito parcial para a obtenção do grau de Bacharel em Direito

Aprovado em ____/____/_____

Banca Examinadora

_____

Professor Orientador

Universidade Tiradentes

_____

Professor Examinador

Universidade Tiradentes

_____

Professor Examinador

Universidade Tiradentes

CRIMES VIRTUAIS: APLICAÇÃO, FALIBILIDADE E IMPUNIDADE

Aldo Maxwell Pereira de Mesquita Caetano

RESUMO:

O presente artigo tem como foco 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[1] espaço virtual e suas peculiaridades, a definição acerca do local de apuração e competência destes crimes nesta modalidade. O estudo tem como objetivo 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.

ABSTRACT:

This article focuses on the application of the Brazilian Penal Code in virtual crimes, and in this context seeks to respond to the problems on the verification and applicability in virtual

[1] *Graduando em Direito pela Universidade Tiradentes – UNIT. E-mail: aldo_maxwell@hotmail.com*

crimes and their possible solutions. So that this problem was solved with the broadest possible relevance short of certain issues must be addressed, like, what it is and, or, cybercrime can be considered, the definition and determination of what would be the virtual space and its peculiarities, the definition of the place of determination and competence of these crimes in this mode. The study is mainly aimed to show how the current measures, better or properly applied in different ways to the current contained in the Brazilian criminal law would punish more effectively. In order to find out how today is dealing with this problem, its implications, facts and issues, current dynamics; thus converging on their applicability and confronting them with the Brazilian legal system, and concluding on their respective efficiency. With glimpse, if so, to adapt these measures, thus improving the efficiency, applicability and use of our criminal law for these criminal practices.

KEYWORDS: Virtual Crimes. Virtual Space. Punishment.

1 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 ate 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 se tornam 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 porque está em presente potência, é um espaço desterritorializante. Esse mundo não é palpável, mas existe de outra forma, 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

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. (MONTEIRO,2007)

Tratando-se de um lado engano pensar que as trocas de informações seriam seguras, afinal o crime é de natureza humana, que sempre esta suscetível à corrupção.

O Direito Penal encontra muitas dificuldades ao tentar adentrar esse domínio. O direito 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.

2 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 esta 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.

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.

Inserido nesse aspecto, e dados os avanços da tecnologia, anteriormente do inicio de uma falta de representação, mostram o momento em que ocorre o aumento de dificuldade na cognição, nas linguagens, na produção do conhecimento.

3 CRIMES VIRTUAIS

3.1. Conceito e Classificação

Também chamados de crimes digitais, crimes eletrônicos, cyber crimes, crimes cibernéticos, entre outras nomenclaturas. São os nomes dados à atividade onde um computador ou rede destes é utilizada como base para cometimento de crimes ou facilitação para destes. Podendo se categorizar esses crimes de acordo com a sua forma de cometimento: os crimes que são cometidos utilizando o computador como instrumento para que se cometa a infração e aqueles que o crime é cometido contra o aparelho em si, o objeto é danificado ou violado de alguma forma (JORGE; WENDT, 2013).

Conceitua Sérgio Marcos Roque como crime de informática sendo: "toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material". (ROQUE, 2007, p.25)

E apesar de sua linguagem pouco tradicional, os crimes associados a estes são de amplo conhecimento e comumente cometidos, tais como roubos, estelionato, chantagem, apropriação indébita, e mesmo outros nem tão comuns, como acesso ilegal a base de dados, interceptação ilegal (por meio de uso de técnicas de transmissão não públicas de dados de computador, para, de ou fora do sistema de computadores), obstrução de dados (danos arquivos de computador, deterioração de arquivos, alteração ou supressão de arquivos de computador), interferência nos sistemas (interferência quanto a entrada e saída de dados, sua transmissão, apagamentos, corrompimento), uso indevido de equipamentos, falsificação de IP's, falsificação de moeda e fraude eletrônica, entre muitos outros

Para Ramalho (2002, apud PINHEIRO, 2006, p.15): [...] os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo, por isso, ficam 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 ou asseclas.

Também se deve levar em consideração o conceito para crime de informática usado pela Organização para a Cooperação Econômica e Desenvolvimento da ONU: o crime de informática é qualquer conduta ilegal e não ética, ou não autorizada, que envolva processamento de dados e, ou transmissão de dados. Ou seja, o crime virtual é toda ação típica, antijurídica e culpável, que através da utilização do objeto tecnologicamente informático conectado à rede mundial de computadores, servindo esta como instrumento ou objeto do delito.

Além destes existem as ações prejudiciais que não são tipificados por lei, tratando-se de algum transtorno ou prejuízo para a vítima, porém sem poder ser atingido criminalmente.

"As "ações prejudiciais atípicas" são aquelas condutas praticadas na/através da rede mundial de computadores, que causam algum transtorno e/ou prejuízo para a vítima, porém não existe uma previsão penal [...]". (JORGE; WENDT, 2013, p.19)

A classificação dos crimes virtuais varia muito em sua nomenclatura acerca dos doutrinadores, alguns as dividem entre crimes ou delitos informáticos próprios, impróprios e mistos; enquanto outros os dividem em crimes cibernéticos abertos e crimes exclusivamente cibernéticos.

3.2 Delitos informáticos

São delitos que apesar das diferentes nomenclaturas dadas pelos diferentes autores todos tratam acerca da maneira de como se dá ou ocorre a perpetração do crime; se este pode ocorrer diretamente sem o uso de computadores ou com eles.

3.3 Delitos Informáticos Impróprios

São aqueles dos quais ocorre a presença ou utilização de computadores, entretanto o bem jurídico tutelado difere da esfera dos crimes virtuais. Podem também serem chamados de crimes cibernéticos Abertos.

Conceitua Dullius, Franco e Hippler que:

> Delitos Informáticos Impróprios podem ser compreendidos como aqueles nos quais o computador é usado, mas não acontece uma violação em algum bem penalmente tutelado, desde modo, para que se caracterize crime, não é necessário um conhecimento abrangente. Exemplos de crimes informáticos impróprios podem ser calúnia (art. 138 do CP Brasileiro), difamação (art.

> 139 do CP Brasileiro), injúria (art. 140 do CP Brasileiro), todos podendo ser cometidos, por exemplo, com o envio de um e-mail. (DULLIUS; FRANCO; HIPPLER. 2012)

E nesse mesmo diapasão:

"[...] crimes cibernéticos "abertos", são aqueles que podem ser praticados da forma tradicional ou por intermédio de computadores, ou seja, o computador é apenas um meio para a prática do crime, que também poderia ser cometido sem o uso dele." (JORGE; WENDT, 2013, p.19)

3.4 Delitos Informáticos Próprios

Já os delitos informáticos impróprios consistem naqueles em que apenas é possível a sua prática quando própria aos crimes virtuais, ou seja, quando o bem jurídico tutelado e atingido for próprio dos crimes virtuais.

Nesse aspecto os delitos informáticos próprios são aqueles em que o bem penal protegido é violado. Exemplo desse crime pode ser apontado a interceptação telemática ilegal, prevista no art. 10 da lei 9296/96.

Assim: "[...] os delitos informáticos próprios são aqueles em que o bem penal protegido é violado." (DULLIUS; FRANCO; HIPPLER. 2012)

Ou mesmo segundo outros autores podem ser também chamados de: "[...] crimes "exclusivamente cibernéticos" são diferentes, pois eles somente podem ser praticados com a utilização de computadores ou de outros recursos tecnológicos que permitem o acesso à internet." (JORGE; WENDT, 2013, p.19)

3.5. Delitos Informáticos Mistos

Os delitos informáticos mistos, podendo também ser chamados de crimes complexos, são aqueles nos quais ocorre a junção de dois ou mais tipos penais.

> Para delitos Informáticos Mistos ou crimes complexos, pode-se afirmar que são crimes que contem a fusão de mais de um tipo penal, em que, além da proteção da inviolabilidade dos dados, a norma visa a tutelar o bem jurídico de natureza diversa. (DULLIUS; FRANCO; HIPPLER. 2012)

3.6. Delitos Informáticos Mediatos ou Indiretos

São aqueles dos quais apesar já existirem e mesclarem dois ou mais tipos penais apenas são possíveis quando da utilização e violação do meio informático, ou seja, um delito informático para que se pudesse consumar crime diverso.

Nesse sentido:

> Os delitos Informáticos Mediatos ou Indiretos, que são conceituados como um delito-fim que não é o de informática, mas adveio do delito-meio informático, realizado para permitir a sua consumação, isso acontece quando uma pessoa transfere dinheiro de uma conta para a outra sem a autorização do titular da conta em que o dinheiro foi sacado, conforme visto, ocorrem dois delitos distintos, o acesso não autorizado a um sistema de computadores, e o furto, sendo um crime de informática que atinge diretamente o patrimônio. (DULLIUS; FRANCO; HIPPLER. 2012)

3.7. Origem

As práticas de crimes virtuais, ou mesmo a definição destes, são recentes, apesar de os computadores serem inventados na década de 40, nos E.U.A., o chamado ENIAC.

O ENIAC começou a ser desenvolvido durante a II Guerra Mundial para computar trajetórias táticas que necessitassem de conhecimentos avançados em matemática, mas apenas passou a funcionar após o fim da guerra e os crimes dos quais chamamos de virtuais, ou mesmo suas respectivas práticas apenas começariam algumas décadas depois.

A história dos crimes virtuais começa por volta das décadas de 50 e 60, com a guerra fria, através de atos de sabotagem e espionagem, dos quais pouquíssimos noticiados, entre a extinta URSS e os E.U.A., sem, contudo ainda existir um conceito mais concreto sobre crimes ou legislação específica para aqueles que o praticavam. Na década de 70, através de parcos conhecimentos em linhas telefônicas sugiram os piratas telefônicos, ou “Phone Phreaks”, que eram capazes de piratear as linhas telefônicas através de dispositivos simples (apitos simples, contidos em caixas de cereal, e capazes de emitir ondas sonoras em determinada frequência a ponto de piratear as linhas telefônicas) e alguns facilmente manufaturados, mas além desta prática eles também roubavam informações das operadoras telefônicas, através da habilidade por eles conhecida como “engenharia social”. Mas as empresas telefônicas e autoridades ao perceberem e entender o que vinha ocorrendo, seus sistemas e abordagens. (KING, 2001)

“**Phreaker:** especialista que utiliza técnicas para burlar os sistemas de segurança das companhias telefônicas, normalmente para fazer ligações de graça ou conseguir créditos.” (CASSANTI, 2014, p.3)

Engenharia social consiste na técnica ou mesmo conjunto de artifícios, com o intuito de fazer a vítima ceder informações ou mesmo utilizar o sistema, seja ele virtual ou telefônico, no intuito de conseguir alguma vantagem, facilidade, ou mesmo acesso quanto ao funcionamento de algum sistema, empresa ou semelhante.

Assim nesse sentido: “É a utilização de um conjunto de técnicas destinadas a ludibriar a vítima, de forma que ela acredite na informação prestada e se convença a fornecer dados pessoais nos quais o criminoso tenha interesse ou a executar alguma tarefa e/ou aplicativo” (JORGE; WENDT, 2013, p.21)

Na década de 80, com a popularização e redução do tamanho dos computadores, os jovens eram encorajados a desmontá-los, roubar seu software e hardware, em seu processo de entendimento e aprendizado sobre computadores (daí vem o surgimento do termo hacker), apesar de que na época em questão os computadores pessoais ainda não tinham muita utilidade, salvo realizar cálculos. Nessa época, ser considerado um hacker não era crime, inclusive essas praticas por eles realizadas eram ate mesmo incentivadas, e se não fossem por eles e seus desbravamentos na área dessa tecnologia não teríamos os avanços e mesmo boa parte das empresas nesse ramo hoje existentes. Foi na década de 90 que realmente chegamos ao conceito de que temos hoje sobre hackers, foi quando começaram a ocorrer os roubos de dados e invasões de maneiras maciças facilitadas pela criação de uma rede integrada, a internet, entretanto esta possuía, e ainda possui inúmeras fraquezas, possibilitando aos hackers cometerem crimes em âmbito global e com muita facilidade; as penas para esses crimes também se tornaram maiores e mais severas, devido ao grande aumento do número de usuários de computadores, da internet e sua utilização e diversificação nas atividades econômicas. (KING, 2001)

3.8. Conceito de crime

O código penal atual não possui uma definição sobre o conceito de crime, deixando esta a cargo da doutrina. Sendo através dela procurado a definição do que seria o ilícito penal. (FABRINI; MIRABETE, 2011)

Crime é todo fato típico, ou ação humana típica que é devidamente inscrita na lei, antijurídica, ou seja, que vai contra essa lei e seja injusta, e culpável. Possuindo como elementos: a conduta (ação ou omissão), resultado, nexo causal ou relação de causalidade e tipicidade. E na ausência de um desses elementos ele se torna atípico, não sendo crime, com exceção da tentativa.

3.9. Lei Penal no Espaço e Local do Crime

No âmbito do Direito Penal é de suma 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, por conseguinte não passível de delimitações físicas, assim interagindo com diversos países.

Quando se pensa na possibilidade do 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.

4 PROCEDIMENTO/PROCESSO CRIMINAL NOS CRIMES VIRTUAIS

4.1. Legislação Específica

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

Esta lei, a 12.735/12, transitou no congresso desde 1999 (PL 84/99, na câmara). Em seu texto original ele 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, sendo reduzidos a dois por veto na sanção, pela presidente Dilma Rousseff.

Ela traz apenas duas mudanças, “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.

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

Ou seja, as polícias civis de todo o Brasil tem 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 contrario, 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)

“A segunda”, inciso II do § 3o do art. 20 da Lei nº 7.716, de 5 de janeiro de 1989 presente em seu artigo 5º, altera o inciso II do §3º do art. 20 da Lei nº 7.716 de 5 de Janeiro de 1989, sobre 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;
>
> .....” (NR)

Já a segunda, 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 obtidos.
>
> § 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.

Como pode se perceber pelo texto da lei, 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, ele 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 comercio 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)

4.2. Como Agir em Casos de Crimes Virtuais.

Os crimes virtuais são punidos da mesma forma que se pune qualquer outro crime, sendo de suma importância que as provas sejam 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).

4.3.Como investigar e apurar judicialmente a autoria.

Como visto só a tarefa de se coletar as informações necessárias em tempo hábil antes que desapareçam é uma tarefa hercúlea. Porém, uma vez feita, começa a investigação que tem por objetivo a descoberta do IP da máquina, e a sua *logs,* que é o seu registro de login, sendo essa a única maneira de se identificar o culpado.

"O log é o equivalente cibernético dos registros mantidos pela companhia telefônica, [...]". (JORGE; WENDT, 2013, p.130)

"Em regra, os registros apresentam a hora de início, duração da sessão, conta do usuário e (para usuários com conexão de discagem, ainda existe) o endereço de IP designado ao computador do usuário para aquela sessão." (JORGE; WENDT, 2013, p.130)

"Toda vez que um usuário digita um endereço no seu navegador de internet ocorre o armazenamento de um registro, [...]." (JORGE; WENDT, 2013, p.130)

Para tanto é necessário a quebra do sigilo telemático, que apenas ocorre após a solicitação da polícia. Primeiro deve-se acionar o provedor de serviços, para que o mesmo envie os dados de conexão (IP, data, hora) que envolvem o suposto crime. Em seguida é acionado o provedor de acesso, e é este que informa os dados físicos do titular da conta de internet que estava conectado no momento que foi identificado o *logs* através do provedor de serviços.

"É através desta correlação envolvendo provedor de serviços e provedor de acesso é possível chegar à autoria de crimes na internet." (CASSANTI, 2014, p.80)

"[...] quem instala uma linha é responsável pelo seu uso. Sendo assim, a princípio o titular é o responsável pelos crimes cometidos no computador." (CASSANTI, 2014, p.80)

5 CONCLUSÃO

Conforme visto em toda a pesquisa, é facilmente constatada a dificuldade tanto de se definir o espaço virtual. E com isso a definição dos crimes virtuais torna-se de difícil avaliação, mostrando-se uma tarefa árdua e cansativa, afinal a difícil limitação de seu território, a facilidade do anonimato, a falta de conhecimento e treinamento por parte das autoridades investigativas, a grande quantidade de crackers e 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.

Além destes, as brechas legais facilmente encontradas na lei, nesse aspecto devendo se salientar a ausência de reserva legal causada pela omissão da lei penal quando da invasão de sistema de informático, se acaso o invasor não objetive fins ilícitos o mesmo não irá vir a ser atingido pela esfera penal, apenas sendo responsabilizado civilmente pelos danos que vier a causar.

A forma de apuração, quando se é vítima destes tipos de delito é de difícil realização, visto que a facilidade de modificação, e grande possibilidade de alterações ou mesmo de se seguir rastros, podendo inclusive por muitas vezes ser confundida a identidade do real autor.

E conforme mostrado a criação de núcleos organizados no intuito do combate aos crimes virtuais não tem se mostrado fácil, muito pelo contrário, tem se mostrado tão difícil e ineficiente que em muitos dos Estados se estão extinguindo os mesmos por falta de estrutura,

pessoal, verba ou mesmo treinamento e capacitação para se trabalhar nesses núcleos, assim estando demonstrando a ineficiência das leis 12.735 de 30 de Novembro de 2012 e a 12.737 de 30 de Novembro de 2012.

E em mesmo sentido leva-se em conta a branda pena que é aplicada nos casos destas respectivas leis, principalmente a Lei 12.737, visto que no Brasil se vislumbra a possibilidade de modificação das penas de até quatro anos de reclusão, quando nos crimes sem violência, por pena de restrição de direitos, assim caracterizando o total descaso para com o assunto, e ao mesmo tempo gerando uma sensação aterrorizante de impunidade e conluio para o crime.

Em suma, para que se houvesse eficiência no combate a crimes virtuais seria necessário se tratar 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 conseguinte, 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.

REFERENCIAS

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

DULLIUS, Aladio Anastacio; FRANCO, Elisa Lunardi; HIPPLER, Aldair. Dos crimes praticados em ambientes virtuais. *Conteúdo Jurídico,* Rio Grande do Sul, agosto. 2012. Disponível em:< http://www.conteudojuridico.com.br/artigo,dos-crimes-praticados-em-ambientes-virtuais,38483.html>. Acesso em 01 de Maio de 2015.

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

JORGE, Higor Vinicius Nogueira; WENDT, Emerson. *Crimes Cibernéticos:* ameaças e procedimentos de investigação. 2 ed. Rio de Janeiro: Brasport, 2013.
ORIGEM dos hackers, A. Direção: Mira King. September Films Production, 2001.

_____. Lei 12.735 de 30 de Novembro de 2012. **Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm> Acesso em: 9 de maio de 2015.

_____.Lei 12.737 de 30 de Novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em 9 de maio de 2015.

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 24 de Abril de 2015.

PINHEIRO, Emiline Piva. *Crimes virtuais: uma análise da criminalidade informática e da resposta estatal*. Disponível em: <www.egov.ufsc.br/portal/sites/default/files/crimes_virtuais_uma_analise_da_criminalidade.pdf>. Acesso em 18 de novembro de 2014.

ROQUE, Sérgio Marcos. *Criminalidade informática:* crimes e criminosos do computador. 1 ed. São Paulo: ADPESP Cultural, 2007.