CENTRO DE EDUCAÇÃO SUPERIOR REINALDO RAMOS – CESREI

FACULDADE REINALDO RAMOS – FARR

CURSO DE BACHARELADO EM DIREITO

JÚLIO VINÍCIUS DE SOUSA BATISTA

A DRÁSTICA EVOLUÇÃO DOS CRIMES CIBERNÉTICOS NO BRASIL E O ACOMPANHAMENTO DAS LEIS ESPECÍFICAS

Campina Grande - PB

2020

JÚLIO VINÍCIUS DE SOUSA BATISTA

A DRÁSTICA EVOLUÇÃO DOS CRIMES CIBERNÉTICOS NO BRASIL E O ACOMPANHAMENTO DAS LEIS ESPECÍFICAS

Trabalho de Conclusão de Curso apresentado ao Curso de Bacharelado em Direito, do Centro de Ensino Superior Reinaldo Ramos, como requisito parcial para a obtenção de título de Bacharel em Direito.

Orientador: Prof. Ms. André Gustavo Santos Lima Carvalho

Campina Grande - PB

2020

B333d Batista, Júlio Vinícius de Sousa.
A drástica evolução dos crimes cibernéticos no Brasil e o acompanhamento das leis específicas / Júlio Vinícius de Sousa Batista. – Campina Grande, 2020.
37 f.

Monografia (Bacharelado em Direito) – Faculdade Reinaldo Ramos-FAAR, Centro de Educação Superior Reinaldo Ramos-CESREI, 2020.
"Orientação: Prof. Me. André Gustavo Santos Lima Carvalho".

1. Crimes Virtuais. 2. Crimes Cibernéticos – Legislação. 3. Direito Brasileiro – Internet – Legislação. I. Carvalho, André Gustavo Santos Lima. II. Título.

CDU 343.2:004.738.5(043)

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECÁRIA SEVERINA SUELI DA SILVA OLIVEIRA CRB-15/225

JÚLIO VINÍCIUS DE SOUSA BATISTA

A DRÁSTICA EVOLUÇÃO DOS CRIMES CIBERNÉTICOS NO BRASIL E O ACOMPANHAMENTO DAS LEIS ESPECÍFICAS

Aprovada em: ___de _____de _____.

BANCA EXAMINADORA

_____

Prof. Ms. André Gustavo Santos Lima Carvalho

Centro de Ensino Superior Reinaldo Ramos - FARR

Orientador

_____

Prof. Ms. Rodrigo Araújo Reul

Centro de Ensino Superior Reinaldo Ramos - FARR

1º Examinador

_____

Prof. Ms. Vinicius Lúcio de Andrade

Centro de Ensino Superior Reinaldo Ramos - FARR

2º Examinador

“Ter acesso ao conhecimento é um presente
de Deus, e saber utilizá-lo, é um privilégio divino”.

(Carmem Garuzzi)

AGRADECIMENTOS

Agradeço, primeiramente, a Deus que me deu energia e benefícios para concluir esse trabalho.

Agradeço a minha mãe que me incentivou todos os anos em que estive na faculdade.

Aos meus colegas de classe que me ajudaram nessa longa caminhada.

Ao meu orientador André, que me auxiliou neste trabalho, sempre prestativo e atencioso.

Enfim, agradeço a todas as pessoas que me ajudaram nessa etapa decisiva de minha vida.

RESUMO

A sociedade foi avançando aos poucos e necessitou-se de um meio que facilitasse o contato entre pessoas em localidades distantes, para acompanhar essa evolução a internet surgiu como uma forma de facilitar a vida das pessoas. A cada ano que se passava os equipamentos que acessam a internet (celulares, computadores, notebooks) foram evoluindo para atender as necessidades das pessoas, conseguindo gradativamente executar tarefas antes realizadas apenas presencialmente. Com isso algumas tarefas antes feitas somente em bancos físicos passaram a ser feitas digitalmente por meio de aplicativos e programas criados pelos mesmos, para facilitar o acesso de seus usuários e garantir comodidade e agilidade na realização de tarefas das agências. Junto com os avanços surgiram alguns problemas, um dos principais é a insegurança, pode, a qualquer momento, mesmo que os usuários utilizadores desses aplicativos e programas não saibam ter alguém mal intencionado com o intuito de ter acesso aos suas informações, para realizar transações bancárias fraudulentas, expor fatos sigilosos de uma determinada empresa, espalhar dados pessoais e íntimos de uma pessoa, manchar a imagem de alguém que tenha um papel importante na sociedade, realizar furtos virtuais. Em virtude de tudo isso é preciso a criação de uma legislação para atender casos de crimes virtuais que estão cada vez mais frequente de ocorrerem, com investimento do governo em delegacias especializadas para atender as vítimas, criação ou alteração de leis para regular as penas desses crimes e sanções mais rígidas para inibir o cometimentos de tais crimes.

Palavras-chave: Crimes virtuais. Tecnologia. Avanço. Legislação. Internet.

ABSTRACT

Society has been advancing little by little and a means has been needed to facilitate contact between people in distant locations, to follow this evolution the internet has emerged as a way to make people's lives easier. With each passing year, the equipment that accesses the internet (cell phones, computers, notebooks) has evolved to meet people's needs, gradually managing to perform tasks previously performed only in person. With that, some tasks previously done only in physical banks started to be done digitally through applications and programs created by them, to facilitate the access of its users and to ensure convenience and agility in carrying out tasks of the branches. Along with the advances some problems have arisen, one of the main ones is insecurity, you can, at any time, even if the users of these applications and programs do not know that someone with malicious intent in order to have access to your information, to carry out bank transactions fraudulent, exposing confidential facts of a certain company, spreading personal and intimate data about a person, tarnishing the image of someone who has an important role in society, carrying out virtual thefts. In view of all this, it is necessary to create legislation to deal with cases of virtual crimes that are more and more frequent, with government investment in specialized police stations to assist victims, creation or alteration of laws to regulate the penalties of these crimes. and stricter sanctions to inhibit the commission of such crimes.

Keywords: Virtual crimes, Technology, Advancement, Legislation, Internet.

SUMÁRIO

INTRODUÇÃO

Durante os anos de 1960 e 1970 aconteceu à revolução das máquinas de calcular, durante esse período surgiu os primeiros teares que utilizavam cartões perfurados, com o passar dos anos foram surgindo diversas inovações tecnológicas, é certo que muitas ocorreram por necessidade humana, com o computador não foi diferente, os primeiros eram enormes até que com o aperfeiçoamento hoje em dia já possuímos máquinas portáteis.

O surgimento da internet no Brasil se deu em torno de 1980 com o desenvolvimento da Rede Nacional de Ensino e Pesquisa e se ampliou para todo o país em 1997. Foi um avanço da raça humana que veio para modernizar o modo de interação entre as pessoas, facilitando a comunicação e tornando-a extremamente mais rápida e aproximando as pessoas, comunicações por cartas que antes demoravam meses para chegar até o destinatário, agora podem chegar instantaneamente.

O surgimento do primeiro computador digital eletrônico foi nos Estados Unidos, criado em 1946, chamado de ENIAC, que quer dizer *Eletronic Numerical Integrator and Calculator*, sua função primordial era manter conexão entre as centrais de computadores dos postos de comando norte americanos.

Estava surgindo ali um novo espaço, chamado de ciberespaço onde não precisava da presença física para se relacionar e trocar conhecimentos bastava apenas que os usuários estivem em torno de uma única linguagem, a informática.

Para os norte americanos era essencial que não houvesse uma rede principal de comando, para que quando ocorresse algum ataque à rede, as demais não ficassem impedidas de manter contato com as que estavam espalhadas em outros postos de comando situados em outras regiões.

Conforme a internet surgiu, os usuários ao longo dos anos foram buscando novas formas de obterem vantagem através de seu conhecimento, normalmente quem faz esses ataques para obter vantagem indevida são hackers que já possuem um considerável conhecimento sobre rede e softwares

em geral e se aproveitam da falta de conhecimento da maioria das vítimas nessa área.

Os crimes virtuais são ilícitos praticados por meio de computadores, notebooks, tablets, celulares, normalmente com intuito de obter vantagem para si ou para outrem ou certas vezes para denegrir a imagem de uma pessoa. Tais crimes permitem que o infrator saia impune na maioria das vezes, pois a rede mundial de computadores permite anonimato e para buscar o infrator pode ser que demande uma investigação para saber sua localidade, endereço de IP, dentre outras formas.

A cada avanço obtido na tecnologia e na sociedade é um novo desafio para ser regulado pelo Direito, quando não possível através do Código Penal surge à necessidade de criação de uma legislação específica para amparar o surgimento das novas situações jurídicas decorrentes das inovações tecnológicas.

Fazer transações de forma rápida e eficaz e na comodidade de sua casa, tudo se tornou mais simples e fácil, do mesmo modo que veio a facilidade de fazer transações, também vieram a facilidade e anonimato para o cometimento de crimes com a ajuda da internet, que atualmente estabelece conexões entre milhares de computadores e celulares ao redor do mundo, concedendo o acesso a diversas informações e compartilhamento de dados de praticamente tudo o que acontece ao redor do mundo.

Diante do exposto do que vem acontecendo no mundo virtual será analisado como o ordenamento jurídico brasileiro está organizado para combater esses ilícitos que estão cada vez frequentes no mundo cibernético.

É necessário o estudo para analisar como se procede a investigação e o combate de crimes onde o anonimato impede a imediata identificação do agente, tornando a investigação bem mais complexa do que normalmente seria no mundo presencial, e como acontece a produção de provas e julgamento desses delitos.

Compreender o que são crimes virtuais e os detalhes dos mesmos contribui para o entendimento do tema, do mesmo modo em que propicia técnicas de aprimoramento para as investigações e caminho para obtenção das provas.

No primeiro capítulo será abordado como se deu o surgimento da tecnologia e o que aconteceu na sociedade com a sua rápida evolução, como ocorria os primeiros crimes cibernéticos e o que foi feito para combatê-los na legislação.

No segundo capítulo é demonstrado como aconteceu à evolução da internet, o que o Direito fez para tentar acompanhar essa evolução e as consequências que ocorreram com a expansão da internet.

O terceiro capítulo será uma explanação sobre como são classificados grande parte dos crimes virtuais e como acontecem na prática e examinar quem são os delinquentes virtuais.

No quarto capítulo será uma análise da Deep Web, como acessar esse “mundo obscuro” e como acontecem os crimes dentro da mesma, será ainda mostrado como funcionam as moedas virtuais e como os criminosos as manuseiam como forma de auxílio no cometimento de crimes virtuais.

No quinto capítulo explorará como as leis nacionais são realmente eficientes na prática para repreender ou impedir a prática desses delitos cibernéticos.

CAPÍTULO I - COMO O DIREITO E A INTERNET SE INTERLIGAM

O direito é uma ciência que deve acompanhar a evolução gradativa da sociedade para poder melhor regulamentar as normas que devem ser seguidas por todos os integrantes dessa sociedade.

Na internet os seus mecanismos de pesquisa têm avançado de maneira gradual desde seu advento, e por isso acarreta-se alguns problemas a quem a utiliza a web é tida como um rápido meio de acesso a várias informações e dados, e se desenvolveu tendo profundas mudanças na vida cotidiana e comportamental do ser humano. Partindo dessa ideia, de agilidade na tecnologia, bem como a facilidade que surgiu em ter acesso a computadores inclusive na palma da mão, vem causando e solidificando novos tipos de relações desde a comercial como também a pessoal.

Com relação a este tema Léa Elisa (2011) nos diz que: “Hodiernamente, então, temos vivenciado uma intensa revolução tecnológica promovida, principalmente, graças a este comentado “mundo de pontas”.. Desta forma, relações pessoais, comerciais, de consumo e de trabalho, entre outras, passam pela rede mundial de computadores, provocando uma revolução jamais vivida pelo mundo até hoje”.

Embora este eficiente meio de comunicação tenha sido criado com o intuito de facilitar e agilizar a vida das pessoas, por muitas vezes é utilizado de forma indevida e ilegal.

Com o advento da internet a sociedade passou a perceber que a mesma faria uma enorme diferença, começando a avançar ligeiramente e entendendo que as novas gerações seriam muito dependentes dela, dessa forma foi substituindo muitas tarefas que antes somente poderiam ser feitas pessoalmente, passando a fazê-las no mundo virtual. Por causa da facilidade de ter acesso à internet em diversas regiões e a utilidade que a mesma possuía, usar a internet passou a ser bem mais vantajoso, seja com economia de tempo, acesso a diversos tipos de promoções ou praticidade e comunicabilidade instantânea com pessoas do seu convívio social, atualmente quem não possui uma rede social ou nem que seja apenas um endereço de e-

mail é considerado isolado da própria sociedade na qual convive, vejamos como TOMAÉL; ALCARÁ; DI CHIARA *pensam sobre o assunto :*

> A configuração em rede é peculiar ao ser humano, ele se agrupa com seus semelhantes e vai estabelecendo relações de trabalho, de amizade, enfim relações de interesses que se desenvolvem e se modificam conforme a sua trajetória. Assim, o indivíduo vai delineando e expandindo sua rede conforme sua inserção na realidade social (TOMAÉL; ALCARÁ; DI CHIARA, 2005, p. 93).

Para compreender essa evolução ao longo dos anos é interessante examinar como e de que forma surgiu à internet, "Network" é uma palavra inglesa que significa "rede". Interligando todas as redes do mundo (militares, universidades, governos, empresas, prestadores de serviços, etc), obtemos uma rede gigante que cobre uma grande parte do planeta. Daí o termo "Inter-redes". Internet é a interconexão de todas as redes do planeta. (NOURIA, 2019) A princípio, veio para ser um tipo de ferramenta “secreta” para manter comunicações no decorrer de guerras e para averiguar o relacionamento entre o homem e as máquinas. Em 1997 foi criada a rede locais de conexão, ampliando-se dessa forma o acesso em todo o território brasileiro. Segundo informações do Ministério da Ciência e Tecnologia em 2011 em torno de 80% da população obtiveram acesso à internet. Neste ambiente existe uma gama gigantesca de informações, essas de uma forma ou de outra inegavelmente atraem dinheiro e este certamente ocasiona a prática de infrações penais. A internet evoluiu de uma forma tão rápida que ainda nos dias de hoje a população humana ainda não está totalmente adequada a forma de se viver com ela, o Direito também ainda não conseguiu regular todas as condutas necessárias para adequar a interação entre o meio presencial e virtual.

Dessa forma, o meio virtual é muito propício para a prática de crimes de todas as espécies, por volta da década de 1980 eclodiu uma imensurável quantidade de crimes de todas as espécies: pedofilia, disseminação de vírus, invasão de sistemas, estelionato... O Estado então deveria tomar alguma providência urgentemente para evitar que o ambiente virtual virasse um caos.

O Direito como ciência jurídica e normatizadora, não iria permanecer inerte a tantas modificações sociais e, desta forma, atitudes ilegais na internet

merecem as devidas tipificações penais, já que essas ilicitudes lesam bens de total importância na sociedade.

Conforme diz Ivette (2005): “A preocupação com essa questão surge nas ultimas décadas com a popularização dessa nova tecnologia, manifestando-se também através da promulgação de leis relativas à informática e na competência privativa da União para legislar sobre a matéria (CF, art. 22, inciso IV) 43”.

A chamada criminalidade seria portanto parte do homem, Émile Durkheim ensina que: “ o delito não ocorre somente na maioria das sociedades de uma ou outra espécie, mais sim em todas as sociedades constituídas pelo ser humano.” O sociólogo francês resume que o delito não só é um fenômeno social normal, como também cumpre outra função.

No mundo cibernético os infratores pensam estar imunes e invisíveis, o que os incentiva a cada vez mais se tornarem experientes e insistentes no que fazem, possivelmente por ser um problema atual na sociedade do século XXI as pessoas menosprezam algo que é de extrema importância nos dias atuais, alguns não compreendem que manter os seus dispositivos seguros diminuíam drasticamente os ataques aos mesmos.

Em meio a todos esses problemas a União começou a se preocupar e na Constituição de 1988 determinou algumas questões relativas a informática que em regra eram de competência dos Estados, o marco inicial das leis que buscaram regulamentar o uso da internet no Brasil foi a Lei 12.965/14 que determinou deveres para quem utiliza e para quem faz a sua distribuição, impôs algumas sanções e termos, que pretendiam buscar melhorar a sua distribuição com uma maior privacidade, segurança e acessibilidade.

Sempre houve a alusão a palavra hacker na esfera penal, de acordo como a internet foi se expandindo é relevante entender de que forma os crimes virtuais vieram a ocorrer, pois rapidamente a internet ficou largamente conhecida ao redor do Brasil, o que levou as pessoas a tentarem usar meios ilícitos para obterem vantagem indevida por meio dela, haja vista que em tudo o que fazemos atualmente sempre existem pessoas tentando trapacear, em torno disso quem comete tais condutas ilícitas é intitulado de “ciber criminoso”.

> Os noticiários dos jornais, praticamente todas as semanas, trazem informações acerca de golpes ou fraudes de ordem econômico-financeiros praticados pela internet, lesando milhares de pessoas. A habilidade dos hackers e crakers no manuseio das ferramentas de informática e de acesso a lugares tidos como intransponíveis por via da internet tem levado as grandes empresas de software e os cientistas da computação a investirem elevados recursos e enorme talento em pesquisas para prevenir as condutas delituosas no mundo virtual (ESCOLA SUPERIOR DO MINISTÉRIO PÚBLICO DE SÃO PAULO, 2002).

Não há sombra de dúvidas que a sociedade atualmente está quase que totalmente dependente da internet, as empresas de vendas não imaginam nunca retroceder a época na qual era necessário ser feita a comunicação com o cliente por carta, a era moderna dos e-mails facilita demais a rápida interação entre loja e consumidor. Investem pesado em marketings, pois atinge uma maior quantidade de público alvo principalmente em redes de streaming como o *YouTube.*

A nossa Constituição assegura o direito a privacidade, portanto esse direito deve ser respeitado, a cerca disso deve haver uma nova legislação que tipifique melhor as condutas infratoras de inviolabilidade de dados para que a privacidade dos usuários possa ser garantida, tentando dessa forma melhorar o índice de transações fraudulentas, de compartilhamento de informações pessoas, vejamos:

> Em face da expansão da internet e, particularmente, do uso de e-mail, a temática da privacidade está na ordem do dia na doutrina jurídica. O direito à privacidade, como supedâneo da personalidade, deve receber proteção jurídica no ambiente virtual, visto que a Constituição Federal assegura a sua inviolabilidade. Por isso, a legislação futura precisa estabelecer os limites protetivos da privacidade no ambiente cibernético, bem como das comunicações em geral e de dados pessoais, inclusive no ambiente laboral, ainda que se verifique eventual utilização indevida ou contrária às normas e determinações da contratação trabalhista e funcional. O empregador poderia ter acesso ou violar correspondência pessoal de seus empregados em decorrência do abuso no uso da internet pelos computadores da empresa? E o sigilo de informações empresariais, na hipótese de empregados repassá-las a terceiros como se correspondência particular fosse? (ESCOLA

> SUPERIOR DO MINISTÉRIO PÚBLICO DE SÃO PAULO, 2002).

Pesando nesse sentido o atual direito eletrônico ainda é difícil de ser regulado pelas leis atuais que possuímos no nosso ordenamento, onde existem condutas que ainda não são totalmente reguladas como vasculhar em máquina alheia, dentre outras onde a regulação ainda é falha devido a pena branda imposta em condutas onde deveria ter um pena mais carrasca, além disso, as leis atuais abarcam quase todas as condutas criminosas possíveis no mundo virtual, tendo em vista a atuação do Código Penal que pode ser de forma subsidiária caso exista algum tipo de lacuna e as Leis 12.735 e 12.737 não abarquem de forma total as condutas criminosas.

CAPÍTULO II - CRIMES CIBERNÉTICOS

Da mesma maneira que a internet e seus avanços se aprimoram com o tempo, igualmente acontece com as engenharias usadas para a prática dos delitos virtuais que ficam cada vez mais “perfeitas” ao longo dos anos graças ao grande avanço constante da tecnologia usada nessa área. Tendo em consideração o vasto número de pessoas utilizando a internet que gira em torno de 4 bilhões, fica cada vez mais complicado descobrir os reais infratores atuantes em cada região específica. Uma ONG registrou durante 11 anos quase 4 milhões de denúncias anônimas sobres crimes cibernéticos, o que indica a baixa segurança nos dispositivos usados para acesso a rede, que os infratores conseguem facilmente burlar e a grande maioria ainda sai impune.

A doutrina diverge entre si em qual local e época ocorreu o primeiro crime cibernético, para ser caracterizado como crime é necessário o uso do computador, pois é uma ferramenta indispensável para a caracterização deste. Para alguns doutrinadores ocorreu nos Estados Unidos no Instituto de Tecnologia de Massachussets em 1964 onde o autor do delito teria sido um aluno, já para outros haveria ocorrido na Universidade de Oxford no ano de 1978, que também teve como autor do delito um aluno o qual teria roubado informações sobre uma prova da universidade. Até aquele momento, não havia nenhuma lei para regular tais crimes, então, a Flórida foi o primeiro Estado onde se teve a iniciativa de elaborar a primeira lei sobre crimes cibernéticos.

Foi realizado na Europa o primeiro estudo sobre crimes cibernéticos tendo como pesquisador Ulrich Sieber. As primeiras evidências de crimes virtuais aconteceram por meio do phising que inicialmente se apoderavam de dados bancários. Ulteriormente, propagou-se uma série delitos espalhando e-mails maliciosos com extorsões, de cunho sexual; como também uma imensa quantidade de materiais envolvendo crianças e adolescentes em sexo explícito. A quantidade de casos levou as pessoas a refletirem sobre a escassez de uma legislação específica que regulasse tais delitos.

O conceito de crime virtual é moderno em comparação aos demais crimes mais frequentes que conhecemos que já foram e são estudados pela

Doutrina há bastante tempo atrás. Com a constante evolução da internet foram inventados novos meios de se cometer velhos crimes, no meio virtual as vítimas são aleatórias e cada dia que se passa é criado uma nova forma de se cometer um delito. De acordo com o advogado Daniel Allan Burg os problemas com os crimes cibernéticos vão além da pluralidade e velocidade no qual se multiplicam, pois a internet facilita a impunidade, uma vez que a investigação é mais complicada e muitas vezes quando o autor é identificado o crime já prescreveu.

2.1 CRIMES VIRTUAIS MAIS COMUNS NO BRASIL

Os principais crimes mais recorrentes no Brasil em meio virtual são: a pornografia infantil; fraudes bancárias; crimes contra a honra: difamação, injúria e calúnia; apologia e incitação aos crimes contra a vida; o tráfico de drogas.

As denúncias feitas sobre pornografia infantil são enviadas para a Policial Federal em razão do convênio firmado com a ONG Safernet, já as fraudes bancárias, as que acontecem com a Caixa Econômica são investigadas pela Polícia Federal , as fraudes com os demais bancos quem fica responsável é a Polícia Civil de cada estado, em cada caso a Polícia Civil instaura um inquérito policial.

Normalmente os crimes contra a honra são investigados pela Polícia Civil, quando ultrapassa os limites nacionais também ultrapassa normalmente a competência da Polícia Civil, dessa forma fica incumbida de fazer a investigação desses casos a Polícia Federal, no caso de tráfico de drogas também é competência da Polícia Federal.

2.1.1 classificação dos criminosos virtuais

Segundo Túlio Lima Vianna (2001) na sua tese de mestrado, os criminosos são classificados de acordo com a sua forma de atuação e o modo no qual pratica os crimes são denominados de:

Crackers de sistemas: são piratas/*hackers* que atacam os computadores interligados em rede;

Crackers de programas: piratas que modificam softwares gratuitos e os fazem funcionar como se fossem pagos, utilizando-se dos programas com todos os recursos disponíveis sem pagar nada por isso;

PHREAKERS: piratas experts em telefonia fixa ou móvel;

DESENVOLVEDORES DE VÍRUS, WORMS e TROJANS: desenvolvedores de softwares com objetivos diversos, que vai desde causar danos às máquinas infectadas até roubar dados e senhas diversas;

PIRATAS DE PROGRAMAS: criminosos que duplicam um programa e burlam os direitos autorais do desenvolvedor original.

De acordo com Vianna (2001) existem diversos indivíduos com capacidades técnicas diversas e motivos inexplicáveis capazes de utilizar a tecnologia para lesar vítimas diversas e alguns deles ainda ensinam aos demais indivíduos que queiram fazer o mesmo e que ainda não conhecem as técnicas adequadas, podem ser classificados de acordo com o que pretendem realizar em:

Vândalos: possuem o intuito de causar apenas algum tipo de prejuízo para as vítimas, desde um simples desligamento da máquina e uma consequente desconexão com a internet, até a total destruição dos dados armazenados na máquina.

Espiões: agem com a intenção de roubar algum tipo de informação sigilosa e útil, como por exemplo, dados sigilosos de um governo, informações e programas militares, uma fórmula industrial secreta de algo que esteja em pleno desenvolvimento...

Revanchista: normalmente são indivíduos que trabalhavam em uma empresa na área de informática possuindo um vasto conhecimento sobre quais as formas que a empresa gerencia seu dia a dia de trabalho, e para causa-lhe algum tipo de prejuízo em forma de vingança resolvem planejar algo para arruinar a mesma.

Pichadores digitais: suas atitudes possuem a intenção de se tornarem reconhecidos no mundo cibernético modificando páginas de internet deixando

nas páginas que foram alteradas sua assinatura ou símbolos que o fazem ser identificados.

Curiosos: atuam apenas por curiosidade e não causam nenhum prejuízo ou mal as vítimas infectadas, possuem intenção de aprender novas técnicas e aprimorar as que já possuem, na maioria das vezes são guiados pela ética existente nos grupos nos qual são vinculados.

Ciber terroristas: são chamados de terroristas digitais, seus estímulos são normalmente políticos, possuindo armas diferenciadas que começam de furto de informações sigilosas, podendo também realizar a queda de sistemas de telefonia e demais ações semelhantes.

Ladrões: suas intenções são claras, invadir sistemas bancários e efetuar desvios de dinheiro para contas bancárias de sua propriedade.

Estelionatários: Possuem assim como os ladrões propósitos financeiros, geralmente buscam conseguir dados de cartões de créditos que estão arquivados em diversos sites de comércio.

2.2 CRIMES VIRTUAIS IMPRÓPRIOS

Os crimes virtuais são denominados impróprios quando o computador é usado para cometimento do crime, porém, não há comprovação da inviolabilidade de nenhum tipo de informação ou dados. Nesse tipo de delito não se necessita de um grande conhecimento técnico para pratica-lo, sendo facilmente praticados por qualquer pessoa com o mínimo de conhecimento, alguns exemplos de crimes impróprios são os contra a honra, dignidade, que podem ser facilmente perpetrados com envios de simples mensagens pelas redes sociais ou ao compartilhar injúria ou difamação de uma determinada pessoa com todos os seus amigos de determinada rede social.

A publicação de mensagens que atentem contra a honra de uma pessoa pelas redes sociais é extremamente fácil de ser feito, sendo possível não apenas atentar contra a honra de uma pessoa, mais também outros delitos como instigação ao suicídio art.122 CP, incitação ao crime art.286 do CP, apologia de crime ou criminoso art. 287 do CP, racismo art. 140, §3° do CP e

Art. 20 da Lei de Crime Racial, falsidade ideológica art.299 do CP, dentre outros.

É chamado de impróprio pelo simples motivo de não haver nenhuma ofensa a qualquer dado informatizado da vítima, crimes desse modelo podem ser facilmente realizados dentro de qualquer página criada exclusivamente para esse fim, dentro da

Deep Web, que é um “mundo” escondido dentro da própria internet, por exemplo, conceito que vai ser explicado melhor adiante, pode-se criar qualquer página com o fim de expor filmagens de cunho sexual de crianças, mas claro, se entrar na Deep Web for um pouco que difícil para iniciantes, pode ser feito facilmente também fora dela, basta criar qualquer página com a intenção de divulgar vídeos sexuais de menores. Sendo assim o crime praticado é o de pedofilia e não foi necessário invadir e nem alterar nenhum dado informático de ninguém, a internet foi apenas um meio utilizado para a divulgação das imagens e consumação do delito.

2.3.1 Crimes virtuais próprios

Os crimes virtuais são chamados de próprios quando os dados informatizados das vítimas são acessados por pessoas mal intencionadas com o objetivo de alterar ou excluir dados em computadores alheios, a interferência em dados informáticos é um tipo de crime próprio que está incluído dentro do crime de acesso não permitido em sistemas informáticos, sendo assim alterar, destruir, impedir o acesso a algum tipo de dado informático significa estar cometendo um acesso não permitido em sistemas informáticos. No Código Penal do Brasil está previsto a modalidade de crime em que o servidor público se valendo da sua condição modifica ou exclui dados informatizados da Administração Pública com o intuito de obter vantagem indevida, o acesso aos dados não é punível, entretanto, é punível a interferência nos dados no decorrer do seu processamento. O intuito do infrator é desestabilizar o correto funcionamento do sistema, gerando anomalias nas máquinas deixando o sistema inoperável. Os dados armazenados no sistema continuam intactos

sem nenhuma alteração, porém fica praticamente impossível de ter acesso aos mesmos com o sistema inacessível.

Normalmente os ataques que são mais constantes é os DOS (Denial Of Service) onde os sites que são atacados permanecem inacessíveis pelos usuários, quando os sites que são atacados trabalham com vendas de produtos os prejuízos são claramente percebíveis em razão da perda de vendas ao ficarem dias ou horas off-line, se não bastasse a perda dos ganhos em relação as vendas, existe outro problema bastante significativo com os compradores, é a perca de confiabilidade em relação ao site aos saberem da vulnerabilidade de segurança que possuem, ficando dessa forma desconfiados em inserir seus dados ao realizarem novas compras futuramente.

No nosso ordenamento jurídico não há previsão sobre o crime de interferência em sistemas computacionais.

Pode-se chamar o crime de interceptação ilegal de crime próprio, pois, os dados no momento em que estariam sendo transferidos de uma máquina para outra são pegos, sendo assim, os infratores não possuem acesso à máquina da vítima, conseguindo obter o os dados durante a transferência entre computadores, sendo muito similar à escuta telefônica onde a comunicação entre os dispositivos é obtida durante o seu tráfego.

O crime está tipificado no art. 10 da Lei 9.296/1996 que descreve: “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.” (BRASIL, 1996).

Não pode esquecer-se do crime de falsificação informática que implica em alteração de dados da máquina com a intenção de burlar algo. Existem várias formas de burlar alterando o registro das máquinas, uma das principais é alterando o registro de programas que são distribuídos em forma de demonstração, sendo um tipo de amostra para que os usuários consigam testa-los e caso gostem possam estar adquirindo o produto pago futuramente, entretanto, os criminosos desenvolvem alguns softwares chamados de cracks, conseguindo dessa forma fazer com que os produtos que antes eram amostras virarem produtos Premium/sem limites de uso alterando ou falsificando o código de registro, fazendo com que o programa ao ler aquele código

adulterado entenda como se fosse um original e o usuário tivesse pagado por ele.

Finalmente, temos também ainda dentro dos crimes informáticos próprios a criação e disseminação de programas altamente arruinadores de sistemas operacionais e máquinas, sendo mais frequentemente chamados e intitulados de vírus. Vírus em latim significa toxina, em biologia são seres parasitas que se implantam em células hospedeiras e nelas se reproduzem rapidamente, de tal forma como os biológicos os vírus eletrônicos se espalham de forma assustadoramente rápida por meio de links e por e-mails na internet. Normalmente são arquivos pequenos em torno de 20 kbytes criados geralmente em linguagem C/CC+, Assembly ou Pascal podem ser facilmente distribuídos por pessoas que enviam emails falsos que se passam por empresas bancárias de renome.

Ainda não temos tipificação de tal crime em nosso ordenamento que objetivasse impedir a criação e distribuição de vírus informáticos, porém já que não existe crime para tipificar a criação e disseminação de vírus, tal ato pode ser enquadrado no crime de dano previsto no art.163 do Código Penal quando o vírus provocar a inutilização de dados contidos no sistema ou causar algum outro defeito na máquina. Mesmo sendo possível enquadrar o infrator no crime de dano seria mais viável que existisse uma lei que tipificasse a condenação pela propagação de vírus como sendo um crime de perigo concreto, pois pode haver um possível dano a máquina ou ao sistema operacional ao fazer a divulgação do mesmo.

2.3.2 crimes virtuais mistos

Crimes virtuais mistos são aqueles que a intenção do legislador ao elaborar a norma não é apenas em proteger a integridade dos dados informáticos, mas, visa também à proteção de outro bem jurídico de valor expressivo. O acesso não autorizado em sistemas eleitorais já foi tipificado pelo nosso ordenamento, sendo que este é um crime que se originou do acesso não permitido em sistemas informáticos, sendo regulado pelo art. 67

VII, da Lei 9.100/95 que assim descreve: “obter ou tentar obter, indevidamente, acesso a sistema de tratamento automático de dados utilizado pelo serviço eleitoral, a fim de alterar a apuração ou contagem de votos.”

Dois anos após essa lei, surgiu a Lei 9.504/97 que no se art. 72, I, regulou o mesmo crime já anteriormente regulado pela lei antecessora assim dispondo: “obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos” (BRASIL, 1997).

Mesmo revogando tacitamente a lei antecessora não houve quase nenhuma mudança, pois a redação de ambas as leis são idênticas sendo que a nova lei nada falou sobre a tentativa, ficando dessa forma ainda existindo efeito da lei antecessora no que descreve sobre a tentativa, o que houve efetivamente foi um aumento de pensa considerável, já que a lei antecessora previa pena de um a dois anos de reclusão, a lei subsequente passou a prever pena de cinco a dez anos de reclusão, isso mostra a gigantesca vontade e preocupação do legislador em punir crimes eleitorais, não sabe ele que tal norma na prática não é muito útil, pois as urnas eletrônicas são muito frágeis em questões de segurança, dessa forma seria quase impossível investigar esse tipo de crime, porque o código fonte da urna não é aberto e não é disponibilizado ao público, dessa forma quem gerencia todo o sistema de votos são os poucos desenvolvedores que possuem acesso ao software desenvolvido para fazer a contagem de votos, podendo esses desenvolvedores fraudar as eleições sem que ninguém consiga saber.

O Tribunal Superior Eleitoral já se posicionou em 2018 em sua nota de esclarecimento alegando que o código fonte não era disponibilizado para evitar ataques ao sistema eleitoral, pois, se o código fonte se tornasse público qualquer hacker poderia tentar fraudar as eleições, todavia isso se trata de uma manobra do Tribunal para que não haja uma rigorosa fiscalização por parte dos partidos políticos, nesse sentido a segurança das urnas eletrônicas não deveriam se basear em um código fonte secreto, mas sim em criptografias de ponta que resguardassem o sistema eleitoral de qualquer tipo de ataque cibernético.

2.3.3 Crime informático mediato ou indireto

Crime informático mediato ou indireto é denominado dessa forma porque serve de delito meio para que se possa atingir um delito principal, o agente só pratica o delito informático em função de almejar praticar o delito fim. Pode-se imaginar um agente que consegue burlar a criptografia do sistema de segurança do banco conseguindo dessa forma transferir qualquer valor para a sua conta bancária, temos o crime informático meio o acesso não permitido em sistemas informáticos que foi usado para que o criminoso conseguisse praticar o delito fim de furto. Nesse sentido será aplicável ao autor do delito a pena prevista apenas para o crime de furto, baseando-se no princípio da consunção onde o crime fim absorve o crime meio. “Em função do principio da consunção, um tipo descarta outro porque consome ou exaure o seu conteúdo proibitivo, isto e, porque há um fechamento material”. (ZAFFARONI et PIERANGELI, 1999 ,p. 735).

Dessa forma o crime fim é classificado como mediado ou indireto quando for aplicável ao caso o princípio da consunção e por consequência não haja punição para o crime meio realizado.

Não se pode confundir o crime informático impróprio com o crime informático mediato, pois em relação aquele existe uma concreta violação aos dados informáticos mesmo que não ocorra a punição em razão do princípio da consunção.

2.3.4 *Sniffers*

São programas normalmente utilizados com intuito de observar o tráfego de dados e ficam em busca de problemas na máquina, em tese eles não são criados para atuar de forma prejudicial, entretanto, armazenam todas as informações da máquina na qual é programado, pode ser instalado em qualquer rede aberta. Nesse sentido os criminosos podem criá-los para obter o maior número possível de dados da máquina da vítima com a finalidade de colher dados bancários e de cartões de crédito fazendo isso quase que de

forma indetectável já que são programas destinados a procurarem erros e problemas na máquina e não são voltados para roubarem informações logo de início, o que pode deixa-los praticamente indetectáveis.

2.3.5 *Cyberbullying*

Pode-se definir o Cyberbullying como sendo a prática do bullying de forma virtual tal acontece na vida presencial, o criminoso se utiliza de computador ou qualquer outro equipamento com acesso ao meio virtual e faz brincadeiras mal intencionadas com a vítima, repetidamente e geralmente utiliza-se de violência psicológica, conforme expõe Cassanti:

> A ação intencional de alguém fazer uso das tecnologias de informação e comunicação para hostilizar, denegrir, diminuir a honra ou reprimir consecutivamente uma pessoa. Contrário do tradicional e não menos preocupante bullying, que é presencial, ou seja, as ações do agressor têm lugar certo, no cyberbullying o agressor não consegue presenciar de forma imediata os resultados da sua ação, minimizando um possível arrependimento ou remorso (CASSANTI, 2014, p. 35).

Como na maior parte dos casos os transgressores se sentem seguros em virtude de terem o anonimato ao seu favor praticam condutas extremamente reprováveis que provavelmente não teriam coragem para fazê-las pessoalmente. A principal característica do bullying virtual é que a mensagem enviada não pode ser facilmente apagada do meio virtual, na grande maioria das vezes mensagens desse tipo quando geram uma grande repercussão mesmo que sejam apagadas pelo usuário criador ainda continua sendo frequentemente compartilhadas pelos demais usuários que normalmente reprovam tais condutas, sendo, dessa forma “inapagável”, pois mesmo que o usuário criador as delete não poderá fazer nada em relação aos compartilhamentos já efetuados antes que a mesma fosse deletada, não podendo impedir a sua propagação.

Nesse sentindo pode-se perceber outro diferencial do cyberbullying em relação ao bullying, no que tange ao possível alcance daquele no mundo virtual, a vítima pode sofrer constantemente as consequências do ato criminoso, porque, como foi perpetrado na internet é impossível calcular o seu alcance, consequentemente não existe como calcular a quantidade de pessoas que tiveram acesso à mensagem compartilhada, ao contrário do bullying que fica restrito ao momento e lugar em que foi efetuado, dessa forma a exposição da vítima do bullying fora do mundo virtual é muito menor.

2.3.6 *Trojan*

Também chamado de “Cavalo de Tróia”, recebeu esse nome em razão da referência que se faz a mitologia grega por ser um vírus que se aproveita de qualquer descuido do usuário infectando o seu sistema operacional de forma em que não seja notado, normalmente é disponibilizado pelo hacker como sendo um programa comum e de uma fonte segura, todavia, no momento em que é executado exibe uma mensagem falsa de erro para fazer o usuário entender que o programa não é compatível com o seu sistema operacional ou em certas ocasiões quando é executado simplesmente desaparece e se infiltra facilmente nas raízes do seu sistema operacional, podendo modificar configurações, alterar registros do Windows, corromper processos essenciais do sistema operacional. Algumas vezes também pode aparecer camuflados o que prejudica ainda mais a sua identificação pelo antivírus, pois o mesmo finge ser um processo essencial para o funcionamento adequado do seu sistema operacional.

2.3.7 Engenharia social

É a forma utilizada em meio virtual para normalmente furtar as vítimas que são enganadas através de métodos persuasivos onde o autor do delito se aproveita do desconhecimento da vítima sobre determinada situação ou valendo-se da curiosidade da mesma sobre determinada notícia faz com que a vítima acredite que o criminoso é uma pessoa de confiança e que é empregado

de qualquer empresa de renome no mercado, o criminoso passa a adquirir a confiança da vítima aos poucos até chegar o ponto em que a vítima acredita que aquela situação que está acontecendo é totalmente real e séria.

CAPÍTULO III - A *DEEPWEB* – O MUNDO OBSCURO DO CRIME

A parte obscura e menos conhecida da internet é denominada de DeepWeb, a grande maioria das pessoas imaginam que a internet que conhecem já é a totalidade do iceberg, não imaginando que por trás dela existe outro mundo gigantesco, muitas delas não conhecem pois a ponta do iceberg ou seja, a internet padrão já consegue suprir as necessidades de grande parte dos usuários. Foram criadas com intenções totalmente diferenciadas a internet convencional é fonte de pesquisa e informação, não passando muito disso, já na Deep Web além de informações é possível fazer muita coisa bizarra e criminosa sem que seja facilmente identificado, pois, ao contrário da internet comum na DeepWeb não se utiliza de DNS e palavras fáceis de se fazerem buscas, para acessar algo localizado na DeepWeb necessita-se saber exatamente o número do endereço da máquina na qual se pretende ter acesso, precisando também de um navegador diferenciado como o Thor para garantir que você não seja um alvo fácil, já que o Thor faz com que sua conexão passe por diversos caminhos até chegar no destino final para que se possa dificultar o rastreamento da máquina em que se está acessando, a logo do navegador Thor ilustra uma cebola em camadas fazendo referência ao caminho no qual o Thor faz com que a máquina percorra até chegar no destino desejado pelo usuário.

O início da DeepWeb foi no ano de 1996 em razão de Paul Syverson ter criado um programa de rede livre e aberta que era capaz de garantir uma maior segurança para seus usuários devido a utilização de inúmeros servidores conhecidos como nós. Dessa forma para cada conexão com o destino pretendido vai se formando pelo caminho vários nós que fazem com que a máquina principal percorra um caminho mais longo até conseguir chegar no destino, porém, com um anonimato muito maior devido a complexidade da conexão. Assim os criminosos viram uma oportunidade única para praticar os crimes sem que pudessem ser facilmente rastreados, tornando da DeepWeb

uma “fossa criminal” propícia a todos os tipos de crimes bárbaros e mais reprováveis possíveis que se possa imaginar.

As transações feitas na DeepWeb utiliza-se normalmente criptomoedas já que não são ainda regulamentadas por nenhum tipo de banco, o que torna ainda mais difícil o rastreamento dos infratores, uma das moedas mais utilizadas é o bitcoin, devido a essas facilidades os criminosos como pedófilos, assassinos de aluguel, terroristas, traficantes de drogas, armas, órgãos humanos se sentem mais seguros e atuam com frequência nesse mercado negro. Também é um local muito seguro para obter informações em sigilo para que os cidadãos não possam saber, os militares podem usar para passar informações sigilosas sem serem descobertos. O crime mais costumeiro na DeepWeb é a exploração sexual de crianças, existem fóruns dos mais variados assuntos, temos fórum somente que tratam sobre exploração sexual de crianças, onde os criminosos publicam diversas fotos e vídeos dos atos praticados pelos menores, onde aqueles são classificados por uma espécie de ranking onde quem posta mais conteúdo sobre o tema que seja relevante para o fórum fica obtendo pontos e quantos mais pontos tiver estará em uma melhor colocação no ranking. Muitas crianças são raptadas na Tailândia, por ser um país miserável, com leis muito brandas, são alvos de criminosos com alto poder aquisitivo que compram muitas crianças devido ao alto grau de pobreza das famílias que sobrevivem passando fome aceitando qualquer valor para entregar as crianças.

Existe também fórum de canibais onde são ensinadas receitas de como preparar uma carne humana, imagens de membros humanos cortados que servirão para o consumo dos canibais usuários dos fóruns.

Alguns fóruns são bloqueados o acesso para conseguir visualizar os conteúdos ali publicados é necessário um pedido de ingresso informando tudo sobre quem pretende ali ingressar, como se fosse uma entrevista, além disso, os moderadores dos fóruns irão fazer uma pesquisa sobre toda a vida da pessoa que pretende ali ingressar, normalmente os fóruns bloqueados são de grupos extremistas que publicam graves preconceitos sobre os grupos que possuem ódio.

Os criminosos precisam fazer a lavagem de dinheiro para transformarem a moeda física que possuem em criptomoedas para conseguirem realizar suas transações no mercado negro tranquilamente, a respeito disso Barbara Calderon explica:

> Se você deseja lavar o seu dinheiro, você precisa trocar o dinheiro que possui (que pode ser em dólar, real, peso argentino, euro, libra esterlina, etc.) por uma moeda que existe apenas no ambiente virtual - como uma espécie de câmbio do novo milênio. Você troca os dólares que possui “comprando” a moeda digital em questão, como, por exemplo, a Bitcoin. Agora você tem uma carteira online recheada de moedas Bitcoins para comprar produtos e serviços na web escura ou, se desejar, trocar por serviços reais como hospedagens em hotéis (CALDERON, 2017, p.80).

Se não bastasse todos esses tipos de criminosos ainda existem os fóruns que tratam sobre vídeos denominados snuffs relativos a homicídios premeditados capturando toda a crueldade que fazem com as vítimas antes de ceifar a vida por completo. Os criminosos mais difíceis de ter contato são normalmente os matadores de aluguéis que são encontrados na parte mais segura e complicada de se ter acesso na DeepWeb, onde é possível encontrar vários matadores de aluguéis e o preço que cobram pelo serviço.

CAPÍTULO IV - LEIS APLICÁVEIS AOS CRIMES CIBERNÉTICOS

Pode-se perceber que grande parte dos crimes cibernéticos já estão tipificados em nosso Código Penal, mesmo que não seja tão simples de identifica-los separadamente, pode-se, pelo princípio da analogia aplica-los em cada caso concreto. O crime de furto, por exemplo, previsto no art.155 com a redação subtrair para si ou para outrem coisa alheia móvel por analogia pode ser adaptável a utilizar dados bancários de outrem para saque de dinheiro com pena de 1 a 4 anos de reclusão, terá a mesma punição o crime virtual, pois se trata do mesmo crime praticado presencialmente. Mesmo sendo possível essa adaptação em grande parte dos crimes virtuais foi muito relevante a entrada em vigência das Leis 12.735 e 12.737, pois com uma lei específica fica mais fácil enquadrar a conduta do indivíduo, garantindo dessa forma uma maior eficiência punitiva. A lei 12.735 veio regular como a Polícia Judiciária ficará organizada para uma melhor efetividade no combate aos crimes cibernéticos, assim dispôs:

> Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado. (BRASIL, 2012)

Na época aconteceram inúmeras críticas a essa lei, pois afirmaram que a mesma era um enorme retrocesso legislativo que tentava impor severas restrições no uso da internet, ficou óbvio na época que essa lei não faria diferença alguma para os criminosos, pois possuíam diversos métodos de praticarem os mesmos crimes sem que a lei os atingisse, quem estava sendo claramente afetados eram os usuários que não iriam poder navegar anonimamente sem colocar os seus dados pessoais em risco, podendo ser monitorados pelas empresas a qualquer momento, tendo os seus dados partilhados entre empresas ou até mesmo vendidos entre elas, por esse motivo estava-se necessitando com urgência da criação do Marco Civil da Internet.

Durante a elaboração da Lei 12.737 ocorreu à famosa invasão da máquina da atriz Carolina Dieckmann, tendo as suas fotos íntimas espalhadas pela internet, por esse motivo a Lei 12.737 recebeu o nome de Lei Carolina

Dieckmann. A referida lei prevê alguns delitos cibernéticos, tais como: invadir dispositivo informático alheio; interromper serviços telefônicos, telegráfico, telemático, informático ou que tenha alguma importância para a sociedade, além da falsificação de documento particular e cartão. Começou-se então a imputar condutas que até então não eram previstas como crimes, mas, muitos ficaram desapontados com as penas brandas previstas nos crimes, não fazendo a principal função da lei que é a prevenção geral negativa.

Percebe-se:

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

A lei especifica que a destruição de dados informáticos sem autorização do dono da máquina é crime com pena prevista de três meses a um ano, não tipificando casos como a invasão de dispositivos alheios com a intenção de pegar as informações e repassa-las para outras pessoas ou empresas, por exemplo, ou se o infrator tiver intenção e curiosidade de apenas ler as informações contidas na máquina será um fato atípico não previsto pela lei, nesse sentido também se por acaso ele não burlar nenhum sistema de segurança não terá praticado nenhum crime se quer.

Fernando Peres explica o processo de criação das leis no âmbito do Poder Legislativo:

> Eu tenho um medo muito grande no processo de criação de leis. Vejo ainda que leis que tratam de áreas específicas como a tecnologia, acabam recebendo muita influência de empresas que possuem algum tipo de interesse. E grandes provedores

> de internet no Brasil, possuem representantes de relações governamentais, que visam impedir que algumas leis sejam aprovadas junto ao Congresso. Agora, na hora de se criarem leis técnicas, apesar de muitas colaborações que recebem , acabam criando previsões que não são inúteis ou são impossíveis de ser realizadas. Como por exemplo, a Lei Carolina Dieckmann, que possui artigos tão específicos, que muitos crimes podem não ser enquadrar. [...] Quando se trata de questão criminal, temos que ser pontuais, não podemos fazer analogias e interpretações em desfavor do réu(PERES, 2017).

Após isso, no ano de 2014 foi elaborada uma nova lei, também conhecida como o Marco Civil da Internet, a Lei 12.965 que pretende gerir o uso correto da internet, por meio de princípios, direitos e deveres para os usuários, essa lei surgiu como objeção a Lei 12.735 de 2012 foi criada em virtude de uma proposta do Poder Executivo para a Câmara dos Deputados, sendo aprovada no dia 23 de abril de 2014, servindo para resguardar a privacidade, determinar como deve ser a utilização dos usuários, garantir a não violação da vida privada, assegurando dessa forma a devida função social da Internet. É norteada segundo princípios como o da reserva jurisdicional, responsabilidade dos provedores, neutralidade, proteção dos dados pessoais, proteção da privacidade, responsabilização dos agentes. A elaboração dessa lei foi de fundamental importância, sobretudo por causa da inserção de responsabilidades na esfera cível para os provedores e usuários.

CONSIDERAÇÕES FINAIS

Pode-se perceber que os crimes cibernéticos continuam em um rápido crescimento, as normas jurídicas e medidas protetivas não possuem capacidade de impedir totalmente essa conduta ilegal que se alastra gradativamente ao longo dos anos.

É perceptível uma falta de interesse por parte das autoridades responsáveis na elaboração de uma nova legislação que consiga abarcar todas as condutas que estão sendo e que venham a ser praticadas no mundo virtual. Sendo assim alguns criminosos ainda conseguem ser punidos, mas em razão das baixas penas impostas aos mesmos, conseguem retornar facilmente para a sociedade para praticar novos delitos, prejudicando muitas pessoas que estão à margem da sociedade que não conseguem se expressar corretamente no ambiente judiciário.

Além disso, as autoridades responsáveis nas investigações dos crimes cibernéticos ainda não possuem equipamentos suficientes para coibir essas práticas que vem se tornando praticamente impossíveis de se impedir e reprimir, muitas vezes ainda conseguem identificar os reais infratores, porém, aquela conduta que foi praticada ainda não é criminalizada pelo nosso ordenamento.

Tais condutas estão se tornando cada vez mais frequentes e os criminosos conseguindo se aprimorarem ainda mais no que fazem, se especializando em ficar o máximo que conseguem indetectáveis, ou seja, fazendo um grande esforço para tentar garantir o maior anonimato possível, está chegando o ponto em que estão se formando diversas organizações criminosas internacionais, sendo um problema mundial e não apenas do Brasil.

Nosso Código Penal é antigo de 1940, nessa época a sociedade evoluiu drasticamente, sendo que os propósitos feitos pelo antigo legislador não são suficientes para abarcar todo o universo virtual hoje existente, dessa forma nosso ordenamento tem que estar em uma constante atualização para que se possa garantir um universo virtual totalmente regulável pelo Direito. Nossos legisladores ainda estão buscando regular todas as condutas que venham a

ser praticadas em ambientes virtuais, sendo plenamente necessário que os estudiosos do Direito busquem entender por completo o ambiente virtual ajudando aos legisladores a entenderem como funciona a nova visão no universo cibernético para que finalmente consigam elaborar novas legislações completas e eficazes.

REFERÊNCIAS

BRASIL. **Código Penal**. Decreto-Lei Nº 2.848, de 7 de dezembro de 1940. Diário Oficial da União. Publicado em 7 de dezembro de 1940.

BRASIL. CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988.
Diário Oficial da União. Publicado em 5 de outubro de 1988.

BRASIL. Lei n.º 12.735 de 30 de novembro de 2012, que tipifica condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares. Diário Oficial da União. Publicado em 30 de novembro de 2012

BRASIL. Lei n.º 12.737 de 30 de novembro de 2012, dispõe sobre a tipificação criminal de delitos informáticos. Diário Oficial da União. Publicado em 30 de novembro de 2012.

CALDERON, Bárbara. **Deep & Dark Web**. Rio de Janeiro. Alta Books, 2017.

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

CALIL, Léa Elisa Silingowschi. **Revolução Digital**. Disponível em: <http://www.mundodosfilosofos.com.br/lea20.htm>. Acessado em: 009. Maio. 2020.

EMILE. Durkheim, Lãs reglas Del método sociológico, Espanha, Morata, 1978, p. 83. (apud) BITENCOURT, Cezar Roberto. Tratado de Direito Penal – Parte Geral, 9ª ed., v. I, São Paulo: Saraiva, 2004.

FERREIRA, Ivette Senise. apud LIMA, Paulo Marco Ferreira. Crimes de Computador e Segurança Computacional. Campinas, SP. Ed. Millennium. 2005.

NOURIA, Lucia Maurity y. **O que é Internet?**
Disponível em: <https://br.ccm.net/faq/12069-o-que-e-internet> Acesso em: 20 de novembro de 2019

ONG registra quase quatro milhões de denúncias de crimes virtuais em 11 anos. Disponível em: < https://esplanadagora.com.br/noticias/acontece/ong-registra-quasequatro-milhoes-de-denuncias-de-crimes-virtuais-em-11-anos>.
Acesso em: 07 de outubro de 2019

PERES, Fernando. Entrevista concedida a Isadora Marina C. de Almeida Pagnozzi. Curitiba, 1 de novembro de 2017

TOMAÉL, M. I.; ALCARÁ, A. R.; DI CHIARA, I. V. **Das Redes Sociais à Inovação**. Ci. Inf., Brasília, v. 34, n. 2, p. 93-104, maio/ago. 2005. Disponível em <http://www.scielo.br/pdf/ci/v34n2/28559.pdf> Acesso em 25 de outubro de 2019

VIANNA, Túlio Lima. **Fundamentos de Direito Penal Informático**. Rio de Janeiro: Forense, 2003.

ZAFFARONI, Eugenio Raúl, PIERANGELI, José Henrique. Manual do Direito **Penal Brasileiro:** parte geral. 2.ed. rev. e atual. São Paulo: Editora Revista dos Tribunais, 1999. 888 p.

ZANELLATO, Marco Antônio. Condutas Ilícitas na sociedade digital, **Caderno Jurídico da Escola Superior do Ministério Público do Estado de São Paulo**, Direito e Internet, n. IV, Julho de 2012.p. 173.