FACER-FACULDADES

UNIDADE RUBIATABA

CURSO DE DIREITO

GRACIELE DE OLIVEIRA GOMES

OS CRIMES CIBERNÉTICOS COM O ADVENTO DA LEI Nº 12737/2012

RUBIATABA-GO
2015

FACER-FACULDADES

UNIDADE RUBIATABA

CURSO DE DIREITO

GRACIELE DE OLIVEIRA GOMES

OS CRIMES CIBERNÉTICOS COM O ADVENTO DA LEI N° 12737/2012

Trabalho de pesquisa apresentado a disciplina de Monografia II do Curso de Direito da Faculdade de Ciência e Educação de Rubiataba-FACER - Sob a orientação da professora Mestre Gloriete Marques Alves Hilário.

De acordo

Professora Orientadora

RUBIATABA-GO
2015

FOLHA DE APROVAÇÃO

OS CRIMES CIBERNÉTICOS COM O ADVENTO DA LEI Nº 12737/2012

Monografia apresentada ao núcleo de trabalho do curso de Direito do Centro de Ensino Superior de Rubiataba-FACER.

Aprovada em, ___ de _____ de 2015.

BANCA EXAMINADORA:

Professora e Orientadora: Prof.ª Mestre Gloriete Marques Alves Hilário

---

Professor examinador: Prof.° Mestre Vilmar Moura Guarani

Professor Examinador: Prof.° Esp. Edilson Rodrigues

AGRADECIMENTOS

Agradeço primeiramente a Deus por me proporcionar a realização deste sonho, por me dar sabedoria e entendimento ao longo desses cinco anos e também por ter me ajudado a manter o equilíbrio todas as vezes que desanimei e pensei em desistir. Agradeço minha irmã Daniela de Oliveira Gomes, que esteve ao meu lado durante esse período, fazendo-me companhia e me dando seu apoio. Não me esquecerei das dificuldades que passamos juntas e das vezes em que ela se privou de coisas para que eu pudesse chegar até aqui. Agradeço aos meus pais Mauro da Rocha Gomes e Maria Lopes de Oliveira Gomes, que tanto me ajudaram. Obrigada mãe pelas suas orações, Deus honrou cada uma delas e hoje posso viver esse momento que para muitos e até mesmo para mim parecia impossível. Agradeço a minha avó, Maria Clarinda Fernandes e ao meu avô Sebastião Lopes de Oliveira (em memória), pelo carinho, amor e pelo apoio que sempre me deram. Agradeço também ao meu noivo, Tiago Oliveira Vitorino pelo cuidado, amor e dedicação, obrigada pela compreensão, por saber entender o quanto a realização desse sonho faria a diferença em minha vida, por saber entender às vezes em que precisei me ausentar e me dedicar primordialmente aos meus estudos. Eu não poderia deixar de agradecer também aos professores e orientadores Martin Manoel Pino Estrada pelo período em que me auxiliou nos estudos e Gloriete Marques Alves Hilário, que se desdobrou para que fosse possível concluir meu trabalho monográfico.

RESUMO: Este trabalho tem como objetivo principal analisar os crimes cibernéticos a partir da edição da lei Nº 12737/2012, abordando as mudanças que esse instituto trouxe a essa modalidade de crimes, cada vez mais comum na sociedade digital. Apresenta-se aqui um breve comparativo entre os crimes digitais antes e depois da edição da Lei Nº 12737/2012, como essa lei surgiu e de que forma ela deverá ajudar a punir criminosos que se utilizam da rede mundial de computadores como meio para cometer crimes. Essa lei surgiu com o intuito de proteger todos os usuários da rede e possui grande relevância para a sociedade por tratar de um tema atual e com aspectos ainda desconhecidos. É importante ressaltar a evolução da legislação brasileira e sua eficácia para coibir os crimes praticados na internet. Muitas infrações podem ser tipificadas como crime cibernético, outras condutas que utilizam a internet como meio podem ser enquadradas no código penal.

Palavras-chaves: Crimes cibernéticos, Internet, Rede, Sociedade digital.

ABSTRACT: This study is meant to examine cyber crimes from the enactment of Law No. 12737/2012, addressing the changes that this institute brought this type of crimes, increasingly common in the digital society. Here is presented a comparative soon between digital crimes before and after the enactment of Law No. 12737/2012, as this law came about and how it should help to punish criminals who use the World Wide Web as a means to commit crimes. This law came about in order to protect all network users and has great relevance to society for dealing with a current topic and still unknown aspects. Importantly, the evolution of Brazilian legislation and its effectiveness in curbing crimes committed on the Internet. Many offenses can be typified as cyber crime, other approaches that use the internet as a means can be placed within the criminal code.

Keywords: Cyber Crimes, Internet, Network, Digital Society.

LISTA DE ABREVEATURAS E SIGLAS

Art.- Artigo

Arts. - Artigos

CP - Código Penal

CPP - Código de Processo Penal

CRFB/88 - Constituição da República Federativa do Brasil de 1988

HC - Habeas corpus

RNP - Rede Nacional de Pesquisas

STF - Supremo Tribunal Federal

STJ - Superior Tribunal de Justiça

PLC - Projeto de Lei da câmara

PLS - Projeto de Lei do Senado

SUMÁRIO

1. INTRODUÇÃO

Esta pesquisa tem por objetivo analisar aspectos relacionados aos Crimes Cibernéticos com o advento da Lei 12.737 de 2012, que tipifica como crimes infrações relacionadas aos meios eletrônicos, como invadir computadores, violar dados de usuários ou "derrubar" *sites*. Definindo também como crimes cibernéticos qualquer tipo de atividade ilegal que usa a internet, uma rede pública ou privada ou um sistema de computador doméstico.

Existem modalidades diferentes de crime cibernético, onde algumas se ocupam de obter informações confidenciais para uso não autorizado e outras se ocupam em invadir a privacidade do máximo possível de usuários de computadores. Essa invasão quase sempre ocorre para fins ilícitos, com objetivo de obter vantagens.

A justificativa da escolha do tema é que o crime cibernético também inclui crimes tradicionais, mais que utilizaram a internet como meio, tais como crimes contra a honra; por intimidação; fraudes de telemarketing e internet; roubo de identidade e roubos de contas de cartões de crédito são considerados crimes cibernéticos quando as atividades ilegais forem realizadas com o uso de um computador e da internet. É um tema atual e que desperta muitas dúvidas da sociedade como um todo e gera discussões doutrinarias quanto a sua eficácia.

O projeto que originou a lei (PLC 35/2012) foi criado Pelo Deputado Paulo Teixeira, com a contribuição de outros deputados, na época em que fotos íntimas da atriz Carolina Dieckmann foram copiadas de seu computador e divulgadas na rede mundial de computadores. O texto era reivindicado pelo sistema financeiro, devido á grande quantidade de golpes aplicados pela internet.

Essa lei altera o Código Penal e tipifica como crime vários delitos cibernéticos. Um exemplo disso é a violação indevida de equipamentos e sistemas conectados ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização do titular, ou ainda para instalar vulnerabilidades.

Crimes “menos graves”, como “invasão de dispositivo informático”, podem ser punidos com prisão de três meses a um ano, além de multa. Condutas mais danosas, como obter pela invasão conteúdo de “comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas” podem ter pena de seis meses a dois anos de prisão, além de multa. O mesmo ocorre se o delito incidir a divulgação, comercialização ou transmissão a terceiros, por meio de venda ou repasse gratuito, do material obtido com a invasão.

A lei prevê ainda o aumento das penas de um sexto a um terço se a invasão causar prejuízo econômico e de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos. As penas também poderão ser aumentadas de um terço à metade se o crime for praticado contra o Presidente da República, Presidentes do Supremo Tribunal Federal, da Câmara, do Senado, de Assembleias e Câmaras legislativas, de câmaras municipais ou dirigentes máximos da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Quanto á problemática da pesquisa esta se baseia no fato de que o delito cometido através da rede torna mais difícil a identificação do sujeito ativo da ação, sendo que os dados do agente podem ser facilmente camuflados, diante disso podemos indagar se realmente se fazia necessária a criação de uma lei que aborda o meio de cometimento de crimes já tipificados no código Penal, ou ainda mesmo, se ela realmente é eficaz ou se foi criada apenas como uma forma de dar resposta à sociedade e a mídia.

A metodologia utilizada foi a de compilação através de pesquisas bibliográficas e documentais, com o auxílio de doutrinas, artigos jurídicos, revistas e internet. A técnica foi a hipotético dedutiva, na forma qualitativa.

2. O SURGIMENTO DA INTERNET E OS CRIMES CIBERNÉTICOS

A internet teve origem nos Estados unidos no ano de 1969, através de um projeto do governo com nome de "*Arpanet*" (*Advanced Research Projects Administration*). A princípio ela era de uso exclusivo dos militares.

> No ano de 1973 realizou-se a primeira conexão internacional da *Arpanet*, que interligou a Inglaterra e a Noruega. No final dessa década a *Arpanet* substituiu seu protocolo de comutação de pacotes, denominado *network Control Protocol* (NCP), para *Transmission Control/ Internet Protocol* (TCP/IP). (Wendt; Jorge, 2013, p.7).

A internet que conhecemos hoje foi criada no decorrer da década de 80, onde "foi implementado, no ano de 1986, a NSFNET- pela *National Science Foudation*-, e a *Arpanet* passou a ser chamada de internet". (WENDT; JORGE, 2013, p.8). Nesse período o mundo começou a se interligar para fins comerciais.

Nos anos 90 houve uma abertura da rede para empresas, onde era permitido somente o uso para expansão do comércio. Nesse período, a internet se tornou uma ferramenta indispensável no cotidiano social surgindo assim um novo ambiente que merece regulação como outros grandes meios de comunicação.

Normalmente são utilizadas algumas nomenclaturas para se referir ao meio de comunicação chamado internet. *Cyberspace,* ou espaço cibernético referem-se á um meio, e não á um lugar ou espaço físico.

A internet surgiu no Brasil em 1988, introduzida pela Rede Nacional de Pesquisas RNP, com o intuito de interligar as redes das universidades com os centros de pesquisas. No entanto, o ministério de comunicações e de ciência e tecnologia só permitiu que ela fosse comercializada em 1995, por meio só RNP e depois com a Embratel.

Ressalta-se que a internet em questão não é *world wide web* ou WWW, esta nasceu em 1989 e foi um elemento essencial para a popularização da internet tornando-a mais acessível.

O termo "cibernético" normalmente é utilizado como sinônimo de informática ou computação, no entanto ele tem um significado próprio. Cibernética estuda formas de controle e leis comportamentais, naturais e sociais. Ela tem como instrumento tanto a ciência da computação quanto a informática, dentre outros.

Os crimes cometidos através da internet não possuem uma nomenclatura única, os crimes cibernéticos também podem ser denominados como crimes eletrônicos, crimes virtuais, crimes digitais, crimes tecnológicos, crimes informáticos, delitos computacionais, etc.

Os crimes virtuais começaram a ser assim reconhecidos por volta da década de 1960, quando a imprensa começou a divulgar os primeiros casos de uso do computador para praticas delituosas, tais como espionagem, manipulação, entre outros. No entanto, só depois de cerca de uma década que a matéria começou a ser estudada de forma mais específica.

2.1. A internet e o direito penal

Com a era digital, o direito encontra-se diante de uma nova realidade. Nesse contexto podemos dizer que vivenciamos o Direito da Informática. "A preocupação em proteger a segurança da informação dos usuários da internet fez-se presente, tendo em vista a ausência de segurança total na sociedade informatizada como ocorre em nosso meio social". (SERRO; SOTO, 2014, p.125).

É pertinente ressaltar que na matéria de Direito Penal e Processual Penal, até o ano de 2012 não possuía legislação especifica para regulamentar as relações na internet, tornando este meio propício para a realização de crimes e condutas lesivas aos seus usuários.

Amâncio (2013, p. 25) explana sobre esta influência da informática a serviço do crime:

> Com o surgimento da internet, surgiu também uma nova comunidade virtual, composta pelos seus usuários, que usam a rede para lazer, pesquisa, trocam informações e trocam negócios. O mundo passa a viver então, na era da informação. O montante de informação veiculada na rede, que corre o mundo em segundos, surpreende até os mais cépticos. Mas juntamente com o desenvolvimento tecnológico, novas modalidades de crime surgiram. O crime de rede, aquele cometido via internet e com o auxilio de computadores, mostra-se sempre dinâmico, na medida que esta em constante atualização e mutação, caminhando junto com os avanços da internet.

A evolução digital tornou possível o surgimento de um novo meio para práticas lesivas, crimes que já faziam parte do nosso ordenamento jurídico ganharam um instrumento mais moderno e eficaz na sua execução. Alguns juristas atenta-se para o surgimento de novos bens jurídicos violados quando as contravenções são cometidas via internet.

Ainda sobre esse tema, Silva (2012, p.123) explana:

> Ocorre que, com as facilidades e trocas de informações, atualizações imediatas e deslumbramento por descobertas pela rede mundial interconectada, os criminosos também vêm se atualizando e modernizando-se constantemente, adaptando-se para concretizarem finalidade ilícitas com modernos e complexos *modus operandi*. Surgiram golpes praticados via rede, como furto de senhas eletrônicas e sua utilização para transferência de valores, disseminação de vírus, crimes contra a honra e condutas praticadas para corromper dados e informações.

A internet veio para diminuir o tempo e o espaço do mundo real. Esse meio de comunicação oferece inúmeras possibilidades, em contraparida ele também expõe as pessoas e torna seus dados mais acessíveis. Esse fator fez com que a legislação vigente caminhasse ao encontro de novas regras de uso da rede, com o objetivo de torna-la mais segura para seus usuários.

2.2. Dos crimes cibernéticos

A maioria dos autores define a internet como uma grande rede que interliga computadores pelo mundo, diminuindo tempo e espaço, espalhando informações de forma eficiente e rápida.

A internet pode ser definida também como a maior rede de comunicação que interliga usuários do mundo todo por meio de computadores. Essa ligação ocorre simultaneamente em vários países que compartilham informações e serviços.

Reis (2013, p. 33) define internet da seguinte forma:

> A internet é um conjunto de redes de computadores ligados entre si através de roteadores e *gateways*, cujo principal objetivo é transmitir informações, diminuindo as distancias e dissipando as fronteiras traçadas pela geografia. A internet instituiu um processo de globalização e diminuição das distancias.

Ou seja, a internet veio como uma forma de diminuir tempo e distancia, ligando pessoas do mundo todo através de seus sistemas. O dicionário Aurélio define a internet como: “Rede mundial de computadores interligados por meio de programas especiais, servidores e

provedores de acesso, e que oferece serviços como *e-mail*, acesso a *sites*, *download* de programas, etc.”

A internet exerce uma influência muito grande na vida das pessoas, “a sociedade e seu espelho regulador que é o poder legislativo parece perdida em meio a revolução tecnológica” (MOREIRA, 2014, p. 16). A internet é um importante meio de comunicação, utilizada tanto para fins pessoais quanto profissionais, ela modificou as relações interpessoais, e o mundo virtual passou a fazer parte de diversos campos, criando novos mecanismos onde a vida e as informações das pessoas estão cada vez mais expostas, criando um ambiente propicio para as práticas delituosas.

Ainda segundo Amâncio. (2013, p. 24 e 25):

> A informática influenciou mudanças em todos os níveis de sociedade. Alterou as relações de amizade e de emprego, que se tornaram virtuais, [...] A sociedade tornou-se outra a partir da evolução e acesso a tecnologia. Os países, as empresas e as pessoas passaram a ter mensuradas suas riquezas, também, pelo nível de acesso á tecnologia e pela capacidade em utilizar-se das informações recebidas para o crescimento econômico e, consequentemente, social.

Essa evolução provocou mudanças no direito obrigando-o a evoluir com a sociedade para cumprir o seu papel de proteger. De acordo com SERRO e SOTO (2014, p.125), “todos nós estamos interconectados diariamente por diversas formas e muitas vezes sem perceber, tendo em vista que o fenômeno digital tem se tornado quase natural”.

De tal forma, até mesmo aquelas pessoas que não possuem acesso direto à internet estão sujeitas a ter seus dados na rede. É impossível estar inserido na sociedade atual sem estar de alguma forma conectada á esta rede, o simples fato de criar cadastro físico em uma loja faz com que sejamos inseridos em um banco de dados digital.

O delito informático é uma conduta típica e ilícita, pode tratar-se de um crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, o seu sujeito ativo pode ser tanto pessoa física quanto jurídica e é cometido utilizando da informática como meio para a pratica.

Dessa forma, pode-se dizer que crime cibernético é aquele que utiliza o computador, ligado ou não á rede, como meio para a prática delituosa. O cibercrime pode ser cometido não apenas por pessoa física, mas também por pessoa jurídica.

Pode-se dizer que além de auxiliar no surgimento de novas modalidades criminosas, a cibernética aprimora, moderniza e potencializa a prática de delitos já existentes, como por exemplo, o estelionato. Ele atrai mais adeptos por sua característica de não ser cometido de forma física, mas virtual, dificultando assim a identificação do sujeito ativo.

A internet é um meio moderno e que proporciona aos criminosos muitas formas para o cometimento de delitos e consequentemente mais eficácia na lesão de bens jurídicos, aqui são tratados os mesmos crimes, mas com um meio novo para sua pratica.

2.2.1. Sujeitos dos crimes virtuais

No ambiente virtual, as pessoas gozam uma liberdade que elas não possuem no mundo real, oportunizando aos usuários a possibilidade de assumir características de gênero, idade e religião ilimitadas. Desse modo, pode-se dizer ou não a verdade sem nenhum prejuízo.

Essas infinitas possibilidades tornam ainda mais difícil identificar e consequentemente punir o invasor criminoso. Em tese, o acesso ocorre através da conexão por roteador, mas o IP será da máquina cadastrada no roteador e não do computador que se conecta ao sinal. O segundo grande problema é a correlação, em um determinado espaço de tempo, entre a máquina e o sujeito que a operador.

A investigação de um cibercrime dever ocorrer de forma permanente para que seja efetuada prisão em flagrante. Se não forem observados os requisitos necessários, essa investigação ensejará em ausência de materialidade e autoria, colocando fim ao processo por falta de uma das condições da ação penal.

Como em qualquer outro crime, no digital o **sujeito ativo** é aquele que pratica a conduta descrita no tipo. Ele não exige nenhuma característica especial para seu enquadramento, portanto o sujeito ativo “pode ser qualquer pessoa, pois, em se tratando de crime comum, não requer nenhuma condição particular” (BITENCOURT, 2012, P.52). Deve-se aqui salientar que aquele que tem autorização para acessar os dados dos dispositivos não poderá ser enquadrado nesse crime.

Por se tratar de crimes na rede, nem sempre é possível identificar o sujeito ativo ou autor do crime, por isso se fez necessário à criação de um perfil de grupos que praticam crimes virtuais, dentre tais denominações está a figura do *hacker*.

Para a identificação do sujeito ativo é necessário também obter informações como, por exemplo, o endereço da máquina, ou seja, o IP, seu *login* e senha, esses dados podem facilmente ser camuflados ou adulterados dificultando a rápida identificação do autor do crime.

São apresentadas algumas nomenclaturas especiais para os criminosos da rede, as mais conhecidas são:

O *cracker*- é aquele que utiliza de seus conhecimentos informáticos de forma ilegal para fins ilícitos em seu proveito ou de outrem, burlando sistemas de segurança e furtando informações sigilosas.

O *reaker*- é aquele que se utiliza de meios de comunicação para uso próprio, e não tem como objetivo causar danos aos demais usuários, ele apenas desafia seus conhecimentos como forma de provar que dominam a rede.

O *lammer*- é aquele que pretende se tornar *Hacker*, ele invade sites. Já o *guru* é o mestre dos *Hackers*, e domina vários sistemas.

As pessoas normalmente confundem o *hacker* com *cracker*; o primeiro apesar de possuir muito conhecimento não causa danos a terceiros, ao passo que o *cracker* é aquele criminoso que usa seus conhecimentos para lesar e cometer crimes.

Existem métodos utilizados para o cometimento de alguns crimes cibernéticos, dentre eles pode-se destacar: Os vírus, capazes de destruir ou alterar dados; O cavalo de troia, que é um programa que uma vez instalado é capaz de subtrair dados, senhas, etc. Os *Sniffers*, espiões que interceptam informações da rede; O *Spyware* que também é um espião que monitora os hábitos do computador e transmite a terceiros.

Quanto ao **sujeito passivo** é aquele tido como o titular do dispositivo. É o proprietário ou em algumas situações o usuário do dispositivo informático. No caso de usuários que não são proprietários do dispositivo pode-se citar, por exemplo, aqueles computadores utilizados por vários membros da família ou no ambiente de trabalho, onde cada um tem o seu perfil e suas senhas individuais.

O sujeito passivo pode ser qualquer pessoa, física ou jurídica, ou entidade titular, seja público ou até mesmo privada. A maioria dos crimes praticados pela internet ainda não são

divulgados, exemplo: muitas empresas evitam denunciar possíveis ataques virtuais ou até mesmo invasões por acharem que isso transmitiria uma imagem de vulnerabilidade em seu sistema de segurança.

2.2.2. Crimes virtuais próprios e impróprios

Os escritores Wendt e Jorge (2013, p.19) classificam os crimes virtuais da seguinte forma:

> Os Crimes Cibernéticos se dividem em crimes cibernéticos abertos e crimes exclusivamente cibernéticos. Com relação aos 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 pratica do crime, que também poderia ser cometido sem o uso dele.

A nomenclatura utilizada por esses autores referem-se a crimes cibernéticos abertos como impróprios e crimes cibernéticos exclusivamente cibernéticos como próprios. Mudam-se apenas os nomes, mais o significado é o mesmo. Essa classificação doutrinária é a mais aceita acerca dos crimes virtuais. Tendo como principal característica sua forma didática e também sua aproximação com a realidade.

Os **crimes virtuais próprios** são aqueles em que o sujeito ativo utiliza o computador como sistema informático com o objetivo de executar crimes, tais como invasão de dados não autorizados e demais interferências que atinjam diretamente o software ou hardware do computador**.**

Os crimes virtuais próprios são atos que tem como bem juridicamente protegido a inviolabilidade de dados. Para que um crime virtual se caracterize como próprio ele precisa praticado ou consumado através de meios eletrônicos. Possuindo como bem juridicamente tutelado a segurança dos sistemas, a titularidade das informações e a integridade dos dados da máquina e periféricos.

São exemplos desses crimes: “Invasão de computador mediante violação de mecanismo de segurança com o fim de obter, adulterar ou excluir dados e informações sem autorização expressa ou tacita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem

ilícita; Interceptação telemática ilegal; Pornografia infantil por meio de sistema de informática; Corrupção de menores em sala de bate papo e Crimes contra a urna eletrônica". (WENDT; JORGE, 2013, p. 20).

Os crimes virtuais impróprios são aqueles que utilizam a máquina do computador como instrumento para a prática do ato ilícito que atinge o bem jurídico tutelado. Ou seja, o computador é apenas um dos meios onde se pode praticar o crime, que já possui tipificação, um exemplo disso é a pedofilia que também pode ocorrer através de outros meios.

Nesse sentido, o computador é apenas mais um meio para a prática do crime. Outros instrumentos também seriam capazes de produzir o resultado, o bem lesado deve ser diverso da informática e não computacional. São exemplos desses crimes: "Crimes contra a honra, Ameaça, Pornografia infantil, Estelionato, Furto mediante fraude, Racismo, Apologia ao crime, Falsa identidade, Concorrência desleal e Trafico de drogas". (WENDT; JORGE, 2013, p. 20).

2.2.3. Natureza jurídica

Em princípio, deve-se analisar o conceito de infração penal e de acordo com o conceito, para que o crime se caracterize, três elementos são indispensáveis, eles definem as condutas de uma eventual ação penal e consequentemente sentença condenatória. São esses elementos a tipicidade, a ilicitude e a culpabilidade.

Conforme o entendimento de Gonçalves (2012, p. 42):

> Dessa forma, pode-se concluir que para a teoria clássica o crime é um fato típico, antijurídico e culpável (três requisitos). O dolo e a culpa integram a culpabilidade. O dolo por sua vez, é normativo, pois tem como requisito a consciência da ilicitude. Para essa teoria o crime tem a seguinte estrutura: 1) Fato típico, que tem os seguintes elementos: a- Conduta; b-resultado; c- nexo causal; d- tipicidade. 2) Antijuridicidade: Cometido um fato típico presume-se ser ele antijurídico, salvo se ocorrer uma das causas excludentes de ilicitude previstas na lei. 3) Culpabilidade, composta pelos seguintes elementos: a-Imputabilidade; b-Exigibilidade de conduta diversa; c- Dolo e culpa.

Partindo da ideia que ocorra um cibercrime, pode-se dizer que um fato que se enquadre nesse estereotipo seja típico, em tese, ilícito e culpável, e que, além disso, seja lesivo a um bem jurídico protegido pelo ordenamento jurídico.

A tipicidade, antijuricidade e a culpabilidade são elementos essenciais para configuração de um crime. Eles estão interligados de tal forma que o elemento posterior do delito pressupõe o anterior. Um ato depende integralmente do outro, de maneira que não será caracterizado crime caso algum desses elementos não se faça presente.

2.2.4. Tempo e lugar dos cibercrimes

A internet, através de sua expansão, rompe com todos os limites territoriais e nacionais na prática de crimes. O espaço virtual proporciona aos seus usuários o livre acesso internacional e também á dados remotos, através de uma "teia virtual".

Dessa forma, afirma-se que durante uma investigação policial acerca de crimes virtuais, deve-se levar em consideração normas do Direito Penal e Processual Penal, e ainda as disposições de Direito Internacional Penal.

O direito internacional pode ser visto como parte integrante do direito penal, a lei nacional regula os atos de uma pessoa onde quer que ela esteja mesmo em países estrangeiros.

Através do princípio da territorialidade, "a lei penal só tem aplicação no território do estado que a editou, pouco importando a nacionalidade do sujeito ativo ou passivo". (GONÇALVES, 2012, p. 36). Fatos ocorridos dentro de um país deverão ser regidos pelas leis desse mesmo país, os Estados exercem a sua soberania dentro e de acordo com os limites do seu espaço territorial.

No princípio da universalidade é o estado do autor ou bem jurídico lesado quem aplica a lei, isso independe do local de cometimento do delito. Este princípio possibilita uma sansão ou responsabilização de forma global, por diferentes Estados, de crimes como se fossem objetos de tratados ou convenções por todos ratificados.

No Brasil, este princípio, o da territorialidade está consagrado no artigo 5º, do Código Penal, onde é definido como território nacional o espaço que corresponde não apenas ao espaço físico compreendido entre as suas fronteiras, como solo, subsolo, águas territoriais e espaço aéreo, mas também as embarcações e as aeronaves brasileiras a serviço do seu governo no estrangeiro, ou as mercantes e privadas que se encontrem em alto-mar.

A teoria da ubiquidade é a que predomina atualmente para a definição do lugar do crime.

Capez (2007, p.102) traz que:

> Teoria da ubiquidade ou mista: Lugar do crime é tanto o da conduta quanto o do resultado. Será, portanto, o lugar onde se deu qualquer dos momentos do *inter criminis*. Essa teoria é também conhecida por teoria mista. Observa-se que os simples atos preparatórios não constituem objeto de cogitação para determinar o *locus delicti*, pois não são típicos.

Nela deve ser entendido como local do crime tanto onde se produziu o resultado quanto local que a ação foi executada. Nos casos em que ação e resultado ocorreram em diferentes países a teoria da ubiquidade traz que a mais adequada é a lei penal no espaço, uma vez que há maior possibilidade de se evitar eventuais conflitos negativos de jurisdição, onde ação e resultado ocorrem em locais diferentes. Essa teoria do lugar do crime encontra-se no artigo 6º, do Código Penal brasileiro.

2.2.5. Bem Juridicamente protegido

A lei 12737/2012 tem como objetivo proteger o bem jurídico que é a privacidade, que tem como espécies a intimidade e a vida privada, valores protegidos pela constituição Federal de 1988 em seu artigo 5º, X que trazem: "São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito á indenização pelo dano material ou moral decorrente de sua violação".

2.2.6. Tentativa e consumação

Antes de tratar da tentativa, devemos salientar que crime é "fato típico e ilícito (ou antijurídico)". (CAPEZ, 2007, p. 114).

Neste sentido, a tentativa seria a execução iniciada do crime, que não se consumou por circunstâncias alheias a vontade do agente, conforme preceitua o artigo 14, inciso II, do Código Penal Brasileiro.

Quando a fase de execução é feita, mas o resultado não ocorre por circunstâncias alheias a vontade do agente, fala-se em tentativa perfeita ou crime falho. No direito existe o chamado "caminho do crime", ou "*inter crimines*".

Este caminho possui quatro etapas: 1° Cogitação; 2º Atos preparatórios; 3º Atos de execução ou Atos executórios - A tentativa está aqui, o agente inicia a execução do crime, mas que não se consuma por circunstâncias alheias a sua vontade; 4º Consumação.

Existem dois tipos de tentativa, a perfeita ou acabada, também chamada de crime falho, quando o agente faz tudo o que está ao seu alcance para consumar o crime, mas isso não acontece por circunstancias alheias a sua vontade. Pode-se falar também em tentativa imperfeita ou inacabada, onde o agente comete somente alguns dos atos de execução, mas e interrompido por circunstâncias alheias a sua vontade.

Essa definição entre tentativa perfeita e tentativa imperfeita irá servir para a dosagem da pena. O crime tentado é punido com a pena do crime consumado, diminuída de 1 a 2/3. O juiz fará essa diminuição levando em conta se a tentativa foi perfeita ou imperfeita.

No ambiente virtual é perfeitamente possível a figura do crime tentado, nos casos em que a conduta do indivíduo que pretende "invadir" um computador alheio apenas com o intuito de visualizar seus e-mails, vasculhando a intimidade alheia. Caso o agente chegue a acessar a caixa postal do titular daquela conta, mas tem sua conduta de tê-la frustrada, não se consumando o núcleo caracterizador do tipo, ou seja, ler a correspondência, configurando-se, assim, o crime tentado. Com tudo, pode- se dizer que ainda em sede de especulações o conhecimento médio em informática e de direito orienta-se no sentido de ser perfeitamente plausível a ideia do crime virtual tentado.

No que diz respeito à consumação, conceituada por NUCCI (2014, p. 175) como "o tipo penal integralmente realizado, ou seja, quando o tipo concreto se enquadra no tipo abstrato". Trata-se está de crime formal, assim o crime se consuma com a invasão e não exige resultado naturalístico. A obtenção, adulteração ou destruição de dados do titular do dispositivo ou até mesmo a instalação de vulnerabilidades não precisam necessariamente ocorrer para que o crime se consuma.

Em regra, para que fique provada a prática do crime de invasão, se faz necessário a comprovação através de uma perícia (art. 158 do CPP).Nada impede também que o delito seja comprovado através de outros meios, como a prova testemunhal (art. 167 do CPP).

2.2.7. Elemento subjetivo

O dolo, acompanhado de um fim em específico para agir, ou seja, um dolo específico. O fim específico de agir desse tipo penal é quando a invasão ocorre com o objetivo de: a) obter, adulterar ou destruir dados ou informações do titular do dispositivo; ou. b) instalar vulnerabilidades para obter vantagem ilícita.

2.2.8. Infração de menor potencial ofensivo

O art. 154-A do CP é crime de menor potencial ofensivo, sujeito à competência do Juizado Especial Criminal (art. 61 da Lei Nº 9.099/95).

Em regra, nos delitos sujeitos ao Juizado Especial Criminal o instrumento de apuração do fato utilizado pela autoridade policial é o termo circunstanciado (art. 69 da Lei Nº 9.099/95). No entanto, nos crimes do art.154-A do Código Penal, quase sempre esse termo circunstanciado não será suficiente para apurar autoria e materialidade do delito, fazendo-se necessário a instauração de inquérito policial e na grande maioria dos casos, será necessária a realização de busca e apreensão na residência do investigado, perícia e oitiva de testemunhas etc.

2.2.9. Das delegacias especializadas em crimes virtuais

Pode-se aqui resaltar que a lei a Lei N.º 12.735/2012, determinou que os órgãos da polícia Judiciária (Polícia Civil e Polícia Federal) devem possuir setores, delegacias e equipes especializadas em delitos na rede, dispositivo de comunicação ou sistema informatizado deverão (art. 4º).

A pena é muito branda, levando-se em consideração a importância do bem jurídico protegido. Em virtude do *quantum* de pena, é frequente a prescrição retroativa pela pena concretamente aplicada. Em Goiás esta delegacia especializada se localiza na cidade de Goiânia (Setor de Analise da Gerencia de inteligência da Policia Civil).

3. A LEI Nº 9. 296/1996 E A CONVENÇÃO DE BUDAPESTE.

Neste capitulo faremos uma analise da Lei Nº 9296 de 24 de julho de 1996, que trata da interceptação telefônica e que antes de ser revogada tacitamente pela Lei Nº 12.737/2012, também regulava acerca dos crimes cibernéticos. Antes de adentrarmos propriamente no estudo da Lei Nº 12.737/2012 é necessário, como estudo introdutório tratarmos da lei de interceptação telefônica de Nº 9.296/1996 que foi o primeiro esboço que tratava acerca da informática e telemática no Brasil.

Falaremos também sobre a Convenção de Budapeste que é o documento internacional sobre cibercrimes que possui relevância no mundo todo, embora o nosso ainda não seja signatário esta convenção serve de norma modelo pra diversos países, inclusive para o Brasil.

3.1. Noções gerais sobre a Lei de interceptação telefônica, Lei Nº 9296 de 1996

Nos últimos anos interceptação telefônica tem sido alvo de inúmeras discussões no meio jurídico e na sociedade civil. Este tema envolve tanto o direito processual quanto o direito criminal e por tratar da intimidade, que é constitucionalmente protegida, envolve também matéria de direito Constitucional. O processo correrá sob segredo de justiça:

Art.1°. "A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observara o disposto nesta lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça".

Segundo o dicionário Aurélio, interceptar significa: "Deter ou interromper em seu curso, não deixar chegar ao seu destino, cortar, por obstáculo no meio de". No direito o significado literal da palavra não é seguido. A interceptação telefônica é o fato de conseguir uma comunicação telefônica, de entrar em contato com uma ligação.

A Lei Nº 9.296/96 se refere a captação e áudio das comunicações telefônicas por parte de uma autoridade competente. Além da transmissão de conversas, a interceptação abrange todo o fluxo de informações transmitido pela informática. Art. 1°. Parágrafo único. "O disposto nesta lei aplica-se á interceptação do fluxo de comunicações em sistemas de informática e telemática".

Antes de analisar a lei de interceptação telefônica, para melhor entendimento, deve-se distinguir escuta, gravação ambiental e interceptação telefônica.

A interceptação telefônica é à entrada de uma terceira pessoa como ouvinte de maneira desconhecida na conversa de dois interlocutores, sem que nenhum deles tomem conhecimento. Segundo a doutrina, a entrada dessa terceira pessoa é indispensável para se caracterizar a interceptação telefônica.

A modalidade de escuta telefônica é aquela onde um dos interlocutores sabe que esta sendo gravado por um terceiro. É a captação da conversa, mas nesse caso com o consentimento de uma das partes.

A gravação ambiental é aquela feita por um dos interlocutores, por isso ela não esta legalmente disciplinada e seu uso dependerá do caso concreto, da forma que foi obtida, se houve ou não a violação da intimidade do outro interlocutor. "Apesar de essa espécie de gravação não

ser tipificada, a prova pode constituir-se ilícita, pois houve violação á intimidade" (RANGEL, 2000, P.78).

Como já foi dito no parágrafo anterior, dessas três modalidades de interceptação, a Lei N° 9.296 de 1996 abarca apenas a interceptação telefônica em sentido estrito, as outras dependem do caso concreto.

3.1.1. Comunicação telefônica

A interceptação é feita sobre uma comunicação telefônica, por meio da informática e da telemática. Este meio é utilizado com a finalidade de apurar crimes e deve ser feito somente com autorização judicial, caso esses requisitos não sejam seguidos, essa prova será invalidada. Entende a doutrina majoritária que é perfeitamente possível à interceptação de comunicações telefônicas e informáticas para o fim de obter provas, essa posição também e adotada dentro dos Tribunais.

Com o advento da lei Nº 9.296/1996 passou a ser permitida a quebra de sigilo das comunicações telefônicas mediante ordem judicial. A interceptação, por ter o único objetivo de produzir provas e por se tratar da invasão pública do privado, deve ser utilizada somente em casos extremos.

3.1.2. Da Prova

A palavra prova deriva do latim *proba*, que é a reunião de atos que tem como objetivo convencer o juiz acerca de alguma coisa, ela é uma forma de demonstração da existência ou veracidade, fundamentada em certo direito que alguém alega ser possuidor.

Para CAMPOS (2014, P.141) a prova é "a demonstração da veracidade de fatos e de alguns direitos, decorrente da atividade realizada pelas partes, através do uso dos meios colocados á sua disposição pelo ordenamento jurídico, sempre com a finalidade de convencer o julgador".

No direito a prova é garantida constitucionalmente pelo devido processo legal. Em regra, quem irá provar é quem alega. No processo penal, quase sempre o Ministério Publico será o autor, assim caberá a ele provar que o acusado foi o autor do delito a ele imputado.

A doutrina majoritária traz que, se for ferida uma norma de natureza processual durante a produção da prova, ela será considerada ilegítima. Tal como a apresentação de documentos ao júri que não foram juntados ao processo com três dias de antecedência.

Desta maneira, pode-se dizer que as provas ilícitas são aquelas produzidas em desacordo com o direito material, assim por mais que sejam importantes para desenrolar do processo devem ser descartadas. Muitas vezes, alega-se a ilicitude da interceptação telefônica. É pacificado hoje que as provas concebidas através da interceptação podem sim ser utilizadas, mais alguns requisitos devem ser seguidos.

As provas ilícitas por derivação são aquelas a que se chegou após um início probatório ilícito. “Existem diversas espécies de provas ilícitas, dentre elas as que atingem a integridade física e psíquica do indivíduo, transformando-se em conduta odiosa e repugnante” (RANGEL, 2000, p.55). Essa prova é considerada ilegal porque deriva de uma forma ilícita, por esse motivo ela não deve ser utilizada com o risco de que contamine o processo como um todo.

Em casos de crime organizado, a produção de provas é bastante dificultosa, a interceptação telefônica é vista muitas vezes como o único meio de obtê-las.

A finalidade da interceptação, como traz o art. 5º, XII da Constituição Federal, é a produção de prova, seja em instrução penal ou investigação criminal, com o intuito de se afastar o princípio da presunção da inocência. A interceptação é feita de maneira cautelar e é uma medida de coação.

Em resumo, a interceptação telefônica é um meio para obtenção de provas, é feita através da gravação ou transmissão, e tem o objetivo de convencer o magistrado quanto á culpabilidade de um agente.

3.2. DOS PROCEDIMENTOS

Quanto aos procedimentos da Lei N° 9.296 de 1996 alguns requisitos devem ser observados, tais como a legitimidade, requerimento, entre outros. A legitimidade de requerer está disposta no art. 3º da referida lei, que denota que a interceptação telefônica pode ser determinada mediante o requerimento da autoridade policial ou de um membro do Ministério Público, durante a investigação criminal ou para a instrução processual penal.

Com base em alguns princípios, a exemplo o do juiz natural, a interceptação não pode ser feita de ofício. A doutrina majoritária entende que o assistente de acusação não esta habilitado á requerer a interceptação. Nos moldes do art. 271 do CPP, ele possui legitimidade para propor meios de prova à autoridade policial ou ao Ministério Público, mas não diretamente.

3.2.1. Do Requerimento

O procedimento tem início com o requerimento, feito pela autoridade policial ou pelo Ministério Público. Ele deverá conter de forma clara a situação que é objeto da investigação, com identificação e qualificação dos investigados, em casos de medida cautelar é necessária a demonstração do *Fumus Bone Jures* e do *Periculum In Mora*.

O *fumus bone jures* se mostrará presente com a demonstração dos indícios de autoria por parte do interceptado. O *periculum in mora* é demonstrado através da impossibilidade da produção de outro tipo de prova, sendo a interceptação a único meio naquele momento. A interceptação é uma exceção, e nunca uma regra.

Para que haja interceptação é necessário também que o crime tenha pena de reclusão. A jurisprudência procurou resolver um problema ao autorizar a interceptação em crimes apenados com detenção, mais isso só seria possível se estes estiverem conexos aos de reclusão.

3.2.2. Do Deferimento

O magistrado decidirá acerca do pedido de interceptação dentro no prazo de até 24 horas, fundamentadamente. Após o deferimento, a interceptação terá início, com a Polícia Judiciária e o Ministério Público, atuando juntos.

O art. 6º da Lei Nº 9.296/96 em seu parágrafo 1° dispõe que “no caso de a diligencia possibilitar a gravação da comunicação interceptada, será determinada a sua transcrição”. Existe certa controvérsia acerca da necessidade de gravar a conversa interceptada. Alguns doutrinadores entendem que essa gravação é facultativa, mais a doutrina majoritária entende o contrário, alegando-se questões de lógica e de celeridade processual. No mesmo artigo, só que em seu 2º parágrafo, a citada lei dispõe sobre a obrigatoriedade das transcrições. A respeito

disso, a jurisprudência do STJ já se manifestou, autorizando a não- desgravação quando a interceptação tiver volume excessivo.

Em caso de indeferimento da interceptação telefônica o Ministério Público poderá fazer uso do recurso de apelação, nos termos do art. 593, inciso II do Código de Processo Penal. O auto circunstanciado citado no art. 8º § 2º da Lei Nº 9296/96 serve também como meio de prova, pois resume as operações realizadas.

3.2.3. Do prazo

O prazo para interceptação é relativo, muitas vezes ele se estende por longos períodos, o que causa bastante furor na mídia e no meio jurídico nacional, pois viola a intimidade dos particulares, em alguns casos, durante anos.

A doutrina dividia-se. Damásio de Jesus, Vicente Greco Filho, Ada Grinover, Antonio Scarance e Luiz Flávio Gomes posicionavam-se a favor de prorrogações ilimitadas enquanto doutores como Paulo Napoleão Quezado, Clarisier Cavalcante e Altamiro Lima Filho pensão de forma contraria.

Existe uma obscuridade na redação do art. 5º da Lei Nº 9.296/96 que traz que "a decisão será fundamentada, sob pena de nulidade, indicando também a forma de execução da diligencia, que não poderá exceder o prazo de 15 (quinze) dias, renovável por igual tempo uma vez comprovada a indispensabilidade do meio de prova".

Como já foi exposto, a interceptação não é uma regra, mas uma exceção. Levando em conta a complexidade dos delitos e das organizações criminosas, bem como a soberania do bem estar coletivo em relação ao individual, esse prazo realmente não pode ser limitado. O entendimento do Supremo Tribunal Federal é favorável e o prazo para interceptação pode ser renovado por mais de uma vez.

3.2.4. Dos crimes da Lei Nº 9.296/1996

Por ser a interceptação telefônica uma absoluta exceção, o legislador buscou inibir a prática de violação da intimidade do particular e resolveu incriminar certas condutas lesivas e

abusivas. O direito á não exposição deve ser respeitado, tendo em vista que “o direito á privacidade materializa-se no direito de estar só”. (ARTESE, 2013, P. 31).

O bem jurídico primordial tutelado no art. 10 da Lei Nº 9.296/1996 é a liberdade de comunicação telefônica, que é a expressão do direito à privacidade. Este artigo derrogou a parte final do inc. II do art. 151 do Código Penal. Outra mudança neste sentido é que os crimes do art. 10 se aperfeiçoam com a mera interceptação, diferentemente do art. 151, II do CP, que exige que a interceptação fosse divulgada.

Trata-se de crimes dolosos, admitindo, no entanto, o dolo eventual, além de coautoria e participação. Quanto as penas elas são rigorosas (reclusão de dois a quatro anos, além de multa), considerando-se que no art. 151, II a pena era de um a três anos, o legislador optou por dar mais ênfase ao direito à intimidade.

3.3. Convenção de Budapeste

A convenção sobre cibercrimes do Conselho da Europa, também conhecida como Convenção de Budapeste, de 23 de Novembro de 2011 é considerado o documento internacional mais importante que trata sobre Direito Penal Informático.

A convenção supracitada serve como norma modelo para regular a cibercriminalidade no mundo todo. Ela tem como objetivos, entre outros: intensificar a cooperação entre os estados-membros, bem como possibilitar a adoção de uma política criminal comum para o combate dos delitos informáticos.

“Alem de normas de direito penal material, que tipificam algumas condutas relacionadas à internet, o referido documento apresenta normas processuais, regulando inclusive, a questão da competência”. (ESTRADA, 2013, p.40).

A convenção de Budapeste divide-se em três eixos, com regras penais (tipificação de delitos informáticos), regras processuais e de cooperação internacional. Estes dispositivos estão

nos arts. 14 a 22, que englobam em seu corpo alguns instrumentos uteis á persecução de crimes informáticos próprios e impróprios e para a obtenção de provas eletrônicas de um crime comum.

Vale ressaltar que o Brasil não e signatário da Convenção de Budapeste, no entanto essa norma é utilizada como modelo para o país. Para se tornar membro é necessário ser convidado pelo Comitê de Ministros do Conselho Europeu.

4. DA LEI "*CAROLINA DIECKMANN*" LEI Nº 12.737 DE 30 DE NOVEMBRO DE 2012

A Lei Nº 12.737 de 30 de novembro de 2012 como já foi falado no capitulo anterior revogou de forma tacita a Lei Nº 9.296/1996, dessa forma ela tipifica como crimes e infrações relacionadas a meios eletrônicos, tais como: Invadir computadores, violar dados de usuários ou "derrubar" *sites* e etc. Popularmente conhecida como "Lei Carolina Dieckmann" ela foi aprovada na época em que a atriz global teve seu computador invadido, e suas fotos íntimas divulgadas na rede, crime tipificado como informático.

A Lei N° 12. 737/2012 surgiu através de um projeto (PLC 35/2012), esse texto era reivindicado devido à grande quantidade de golpes aplicados através da internet.

Foram acrescentados ao código penal os artigos 154-A e 154-B; os artigos 266 e 298 também foram alterados. A lei acima citada teve um período de vacância de 120 dias e entrou em vigor em 2 de abril de 2013.

A presidente Dilma Rousseff promoveu a alteração no código Penal Brasileiro através do Decreto-Lei 2.848 de 7 de Dezembro de 1940. Tal legislação é oriunda do projeto de lei

2793/2011 apresentado em 19 de novembro de 2011, pelo deputado Paulo Teixeira do PT de São Paulo. Seu tempo de tramitação em relação aos outros projetos sobre crimes informáticos foi muito rápido.

A norma abrange a violação indevida de equipamentos e sistemas, estando eles conectados ou não a rede de computadores com fins ilícitos de obter dados e informações, sem previa autorização do titular, ou até mesmo para instalar vulnerabilidades.

Essa lei enfrenta diversas críticas por parte de juristas, peritos, especialistas e profissionais de segurança da informação, pela dificuldade de interpretação de seus dispositivos que são muito amplos; e segundo eles, muitas vezes confusos, tornando a lei injusta e ineficaz.

A Lei n.° 12.737/2012 promoveu as seguintes alterações no Código Penal:

1º– Acrescentou os art. 154-A e 154-B, onde foi inserido um novo tipo penal denominado de "Invasão de dispositivo informático";

2º – Inseriu o § 1º ao art. 266 prevendo como crime a conduta de interromper "serviço telemático ou de informação de utilidade pública";

3º – Inseriu o parágrafo único ao art. 298 estabelecendo que configure também o crime de falsidade de documento particular (art. 298) a conduta de falsificar ou alterar cartão de crédito ou de débito.

4.1. Invasão de dispositivo informático

O art. 154-A da Lei n° 12. 737/2012 trouxe um novo tipo penal, denominado "invasão de dispositivo informático". Vejamos:

> 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.

O primeiro elemento do tipo penal é “invadir”, ou seja, adentrar sem autorização, em determinado local. A invasão a que se refere o artigo é virtual, no sistema ou na memória do dispositivo informático.

O segundo elemento é o “dispositivo informático”. Na informática, dispositivo é o equipamento físico (*hardware*) que tem a função de rodar programas (*softwares*) ou ainda para ser conectado a outros equipamentos, dando a eles alguma funcionalidade.

Outro elemento que compõe o tipo penal é “alheio” que é o dispositivo do terceiro, onde o agente ingressou. Se o dispositivo é de uso próprio, não haverá o crime disposto no artigo 154-A.

Em seguida tem-se “conectado ou não à rede de computadores”. A maior parte das invasões de dispositivos ocorre através da internet, no entanto a lei admite a configuração do mesmo crime em casos em que o dispositivo invadido não esteja conectado à rede mundial de computadores.

Logo, o crime só será configurado caso ocorra à “violação de mecanismo de segurança”. Essa é uma falha grave, pois a privacidade, bem juridicamente protegido pela mesma lei foi violada, no entanto não configura o crime.

Nesta esteira, “com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo”, trata-se da finalidade da ação. Ou ainda, “com o fim de instalar vulnerabilidades para obter vantagem ilícita”, ou seja, é o caso do *cracker* que invade um computador e instala um programa espião com o fim de obter senhas de acesso ás contas em bancos.

4.1.1. Figura equiparada

O seguinte visa discutir acerca da figura equiparada no delito. Logo, o art. 154- A, em seu parágrafo primeiro, estabelece que: “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*”.

Deve-se ressaltar que isso só valerá para os casos em que o fim seja ilícito, casos em que empresas ou escolas desenvolvem programas espiões para testar a segurança ou até mesmo com fins docentes não se enquadram nesse tipo, logo não se configura o crime.

O § 1º menciona tanto programas de computador (*softwares*) como também dispositivos (*hardwares*) destinados à invasão indevida de outros dispositivos informáticos, como é o caso dos chamados "chupa cabra".

Por fim, cabe ressaltar que tanto quem "produz", como quem "oferece", "distribui", "vende" ou "divulga" o programa ou dispositivo é punido. Ou seja, existem inúmeras páginas na internet que divulgam *softwares* espiões e invasores. Essa conduta é crime, punido dentro dos parâmetros da nova lei.

Com a Lei Nº 12.737/2012, esses conteúdos devem ser divulgados com mais cautela, pois se ficar provada a finalidade ilícita do agente que se utiliza do programa para obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita, a conduta passa a ser crime.

4.1.2. Invasão que gera prejuízo econômico (causa de aumento)

O parágrafo segundo do art. 154-A, estabelece que: "Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico". O referido diploma legal traz as causas de aumento de pena, em casos de invasão que gera prejuízo econômico. O parágrafo supracitado é enfático ao dizer que o mesmo não se aplica para o parágrafo terceiro deste mesmo artigo, que será analisado no próximo tópico.

No caso do crime do art. 154-A não é exigido que o invasor tivesse obtido qualquer vantagem, basta que haja a invasão. No entanto, se a vítima sofrer qualquer prejuízo econômico, haverá causa de aumento de pena prevista no § 2º do art. 154-A.

É importante ressaltar que se o prejuízo econômico da vítima for através de valores subtraídos, não haverá o crime do art. 154-A, com essa causa de aumento do § 2º, o delito será de furto qualificado, pois o furto é mais específico que o delito de invasão.

O artigo 154-A, em seu parágrafo quarto e quinto elencam algumas hipóteses ou causas de aumento de pena, previstas para estes delitos. Primeiramente, “Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiros, a qualquer título, dos dados ou informações obtidos.” (§ 4° art. 154-A).

Logo, o referido diploma traz uma causa de aumento específica para o delito previsto no § 3º. Assim, o agente terá sua pena aumentada se além de obter ele divulgar, comercializar ou transmitir a outros o conteúdo contido em: a) Comunicações eletrônicas privadas; b) Segredos comerciais ou industriais; c) Informações sigilosas.

Caso o agente pratique o art. 154-A, § 3º e 4º o delito deixa de ser de competência do Juizado Especial Criminal, considerando que, aplicada a causa de aumento sobre a reprimenda prevista no § 3º o crime terá pena máxima superior a 2 (dois) anos.

Já o parágrafo quinto, estabelece o seguinte:

> § 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.

Ora, o parágrafo 5º acima citado, traz aumento de pena para os casos em que a invasão de dispositivo informático ocorrer contra determinadas autoridades. Esse aumento incide tanto para o crime cometido no caput do art. 154-A como também para a figura qualificada do § 3º.

4.1.3. Invasão qualificada pelo resultado (qualificadora)

A invasão qualificada pelo resultado está prevista no parágrafo terceiro do art. 154-A, o qual estabelece o seguinte:

> § 3º Se da invasão forem obtidos conteúdos 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.

A qualificadora prevista no § 3º do art. 154-A ocorrerá se da invasão, o agente conseguir obter o conteúdo de: a) Comunicações eletrônicas privadas, como e-mails, SMS, diálogos em programas de troca de mensagens etc; b) Segredos comerciais ou industriais; c) Informações sigilosas, sendo que, para qualificar o crime, este sigilo deve ser definido em lei.

Incidirá também a qualificadora no caso do invasor conseguir obter o controle remoto do dispositivo invadido.

O parágrafo supracitado é exemplo expresso da aplicação do princípio da subsidiariedade, levando em conta que o próprio tipo penal prevê que não haverá invasão qualificada se o ato do agente constituir outro crime mais grave. “Havendo duas normas aplicáveis ao caso concreto, se uma delas puder ser considerada subsidiaria em relação a outra, aplica-se a norma principal, denominada “primaria”, em detrimento da norma subsidiaria”.(GONCALVES, 2012, p. 27). Para que esse instituto seja eficaz o interprete deve analisar o caso concreto, verificando a subsidiariedade da norma.

4.2. Ação penal

Quanto aos crimes do art. 154-A em regra, a ação penal ocorre mediante representação, mas existem exceções, nelas a ação será publica incondicionada, como será abordado ao longo deste tópico.

De suma importância, o art. 154-B traz as regras e exceções da ação penal dos crimes definidos no art. 154-A. Vejamos:

> Art. 154-B. Em crimes definidos no art.154-A, procede-se mediante representação, salvo em casos em que o crime é cometido contra a administração pública direta ou indireta de qualquer dos poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Em regra o crime do art.154-A é de ação penal pública condicionada á representação. Isso porque o bem jurídico violado que é a intimidade e a vida privada é disponível, e cabe à vítima avaliar o quanto sua intimidade foi violada, os prejuízos que essa violação causou e se é necessário um processo judicial, ou se as consequências advindas dele poderão ser ainda maiores, expondo sua vida privada de forma ainda mais devastadora.

Assim, é indispensável que a vítima ofereça representação para que seja iniciada qualquer investigação sobre o fato (art. 5º, § 4º, do CPP), bem como para que seja proposta a denúncia por parte do Ministério Público.

Quanto às exceções, o crime do art. 154-A será de ação pública incondicionada caso ele seja cometido contra: a) A administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios; b) Empresas concessionárias de serviços públicos.

4.3. Interrupção ou perturbação de serviço telegráfico ou telefônico, informático, telemático ou de informação de utilidade pública.

A Lei n.º 12.737/2012 inseriu o § 1º ao art. 266 do Código Penal, renumerando o antigo parágrafo único, que agora passa a ser o § 2º. O caput não foi modificado a única inovação está no § 1º, que é analisado agora.

> Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento: Pena - detenção, de um a três anos, e multa. § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

O *caput* do art. 266 do Código Penal não sofreu alterações, no entanto, a Lei N º 12.737/2012 inseriu o parágrafo 1º. O atual parágrafo 2º antes da lei era parágrafo único, e teve

seu conteúdo alterado, antes ele trazia: “Aplicam-se as penas em dobro, se o crime é cometido por ocasião de calamidade pública”. Pela edição da lei, agora ele se apresenta da seguinte forma: “Aplicam-se as penas em dobro se o crime for cometido por ocasião de calamidade pública”.

O art. 266, em seu *caput*, prevê que é crime interromper (paralisar) ou perturbar (atrapalhar): a) serviço telegráfico; b) serviço radiotelegráfico ou c) serviço telefônico. Além disso, também prevê que, se o serviço já estiver interrompido, será considerado crime o fato impedir ou dificultar o seu restabelecimento do mesmo.

Os serviços telegráficos e radiotelegráficos previstos no caput deste artigo estão em desuso. Além do telefone, os serviços telemáticos são os mais utilizados em especial a internet.

Por esse motivo, o art. 266 estava desatualizado, a interrupção de serviço telemático não era prevista como crime. O objetivo da alteração foi, portanto, trazer essa nova incriminação.

Com o novo § 1º, prática o crime do art. 266 do Código Penal quem interromper: a) serviço telemático; ou b) serviço de informação de utilidade pública. Se este serviço telemático ou de informação de utilidade pública já estiver interrompido, também será crime a conduta de impedir ou dificultar o seu restabelecimento.

Se um agente perturbar, mas sem interromper serviço telemático ou de informação de utilidade pública ele não pratica nenhum tipo de crime. A Lei Nº 12.737/2012 foi omissa ao deixar de tipificar a conduta como é feito no caso do caput, para os serviços telegráfico, radiotelegráfico ou serviço telefônico.

4.4. Inserção do parágrafo único ao art. 298 do Código Penal

Através da Lei N° 12.737/2012, foi inserido o parágrafo único ao artigo 298 do Código Penal. Vejamos:

> Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro: Pena - reclusão, de um a cinco anos, e multa. Falsificação de cartão: Parágrafo único. Para fins do disposto no Caput, equipara-se a documento particular o cartão de crédito ou débito.

O principal objetivo dessa alteração foi fazer com que o cartão de crédito ou débito, em matéria penal seja considerado “documento particular”. Desta forma, se o agente não titular da

conta bancária, subtrai um cartão e com ele faz saques bancários ele pratica furto mediante fraude, ficando absolvido da falsificação.

4.5. A Lei Nº 12737/2012 na sociedade digital

Antes da Lei Nº 12.737 de 2012, já existia uma legislação que tratava de crimes informáticos, a Lei de Nº 9.296 de 1996. O art. 10 da mencionada lei trazia que configura crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo de justiça, sem autorização judicial ou por motivos não autorizados em lei, com pena de reclusão de dois a quatro anos e multa. Esta lei foi revogada tacitamente pela de Nº 12.737.

A Lei Nº 12.737 de 2012 é uma legislação que trata especificamente de crimes cibernéticos. Ela criou tipos penais e fez modificações e alterações no código penal. Existe uma duvida acerca da sua relevância, tema que gera muitas discussões e divide opiniões no meio jurídico.

Alguns doutrinadores defendem a sua desnecessidade alegando que o Código Penal já trata do tema por analogia, visto que se trata de crimes comuns, no entanto o bem jurídico protegido é o dado digital, havendo assim uma interpretação extensiva e não uma analogia.

Aqueles que defendem uma legislação específica para tratar de crimes cibernéticos diferenciam os crimes digitais de duas formas: crimes digitais próprios e crimes digitais impróprios. Onde os impróprios são aqueles que utilizam a informática como meio ou instrumento para a prática do crime, são também chamados de crimes comuns. Segundo os defensores desta corrente, estes crimes já estão tipificados na legislação penal. Já os crimes digitais próprios seriam aqueles contra o sistema informacional podendo ser cometidos apenas através deste meio, são elencados como a supressão de dados informáticos, invasão de sistemas, destruição de dados informáticos e fraude de sistemas para obtenção de vantagem ilícita.

Para alguns doutrinadores o Código Penal é totalmente aplicável no âmbito eletrônico, porque ele é só mais um meio para se praticar crimes; a legislação penal no Brasil é suficiente para tutelar as novas condutas, porque as condutas continuam as mesmas, só que ganharam um formato novo.

Essas correntes defendem que Direito Penal nas relações virtuais deve ser mínimo, defendendo que não se faz necessária a criação de uma legislação nova, deve-se usar direito

penal minimamente, usando os outros ramos do direito para coibir as situações praticadas no ambiente eletrônico. Deve o Direito Penal ser guardado e resguardado para situações extremas.

Os que se posicionam contra a criação da Lei Nº 1.2737 de 2012 afirmam que o legislador agiu de forma compulsiva, pois pagar indenização é uma coisa, perder a liberdade é outra e criar muitas leis faz com que o instituto perca sua credibilidade. Sendo que o Código Penal é capaz de enquadrar todas as condutas inseridas com a nova lei, cabendo ao juiz cumprir o seu papel de aplicar a lei no caso concreto.

5. CONSIDERAÇÕES FINAIS

Neste trabalho monográfico foram analisadas as formas de cometimento de crimes no cyber espaço, fazendo comparativos entre os crimes virtuais apartir da Lei 9.396/1996 e as mudanças que a edição da Lei Nº 12737/2012 trouxe á essa modalidade de crimes.

Os crimes cibernéticos estão crescendo de forma tão acelerada que preocupa tanto os que fazem parte do ramo do direito quanto à sociedade como um todo, se tornando cada vez mais necessário o surgimento de uma legislação verdadeiramente eficaz para coibir as práticas delituosas em ambiente virtual. Embora a Lei Nº 12737/2012 possua muitas falhas, ela surgiu com o objetivo de proteger essa sociedade digital, que necessita dos meios eletrônicos em grande parte de seus afazeres.

Alguns crimes virtuais necessitam de meios eletrônicos para que sejam executados, outros apesar de serem cometidos com o auxilio de um computador, podem se consumar através de outros meios. A divergência doutrinaria quanto á necessidade ou desnecessidade de uma lei que trate de crimes cibernéticos esta justamente ai. Alguns defendem que os crimes que só se configuram por meios eletrônicos devem ser tratados dentro de suas especificidades de maneira diferente.

A partir do que foi abordado neste trabalho, pode-se concluir que o surgimento da Lei N° 12.737/2012 de certa forma tornou mais branda as punições de criminosos que utilizam o meio virtual como instrumento para lesar terceiros.

Essa lei possui muitas falhas, um exemplo disso é que o crime só se configura se houver a violação de algum mecanismo de segurança, caso essa invasão seja, por exemplo, de um *pen*

drive que não possui senha, não haverá crime, ainda que a privacidade que é um bem juridicamente protegido tenha sido violada.

Antes o Código Penal já era capaz de tratar todos esses crimes tipificados na Lei Nº 12.737/2012, por analogia ou através da interpretação extensiva. Esse dispositivo aborda apenas o meio para cometimento de crimes já tratados no Código Penal. Devemos considerar que são os mesmos crimes, mais com meios mais modernos e eficazes em seu cometimento.

Devemos considerar também que a edição desta lei é, de certa forma, um meio de acalmar a sociedade e a mídia que desconhecem o ordenamento jurídico vigente, tendo em vista que a criação desta se deu no período em que a conhecida atriz global Carolina Dieckmann teve suas fotos intimas copiadas e divulgadas na rede mundial de computadores.

REFERÊNCIAS

AMANCIO, Tania Maria Cardoso Silva. O impacto do direito na sociedade e o direito no Brasil. **Revista Jurídica Consulex**. São Paulo: Consulex, 2013.

ARTESE, Gustavo. As trancas da lei da internet. **Revista Jurídica Consulex**. São paulo: Consulex, 2013.

BITENCOURT, Cesar Roberto. **Tratado de direito penal: parte especial**. 12 ed. São Paulo: Saraiva, 2012.

CAMPOS, Amália Rosa. **Direito e tecnologia**. Porto Alegre: Livraria do advogado, 2014.

CAPEZ, Fernando**. Curso de direto penal: legislação especial**. 11. ed. São Paulo: Saraiva, 2011.

CAPEZ, Fernando. **Curso de direito penal**. 11. ed. São Paulo: Saraiva, 2007.

ESTRADA, Manuel Martin Pino. Os crimes informáticos na internet profunda e deep web. **Revista Jurídica Consulex**. São Paulo: Consulex, 2013.

FERREIRA, Aurélio Buarque de Holanda. **Dicionário básico de língua portuguesa**. Rio de Janeiro: Nova fronteira, 1988.

GONCALVES, Victor Eduardo Rios. **Sinopses jurídicas: Direito Penal, parte geral**.10 ed. São Paulo: Saraiva, 2012.

MOREIRA, Fabio Lucas. **O Direito na Era Digital**. Porto Alegre: Livraria do Advogado, 2012.

NUCCI, Guilherme de Souza. **Manual de direito penal**. 10 ed. Rio de Janeiro: Forense, 2014.

RANGEL, Ricardo Melchior de Barros. **A prova ilícita e a interceptação telefônica no direito processual penal brasileiro**. Rio de Janeiro: Forense, 2000.

REIS, Wanderlei José. Delitos Cibernéticos: Implicações da Lei N 12.737/2012. **Revista Jurídica Consulex**. São Paulo: Consulex, 2013.

SILVA, Mauricio Faria da. O procedimento investigatório dos crimes praticados pela internet.In: **O Direito na Era Digital.** Porto Alegre: Livraria do Advogado, 2012.

SERRO, Bruna Manhago; SOTO, Rafael Eduardo de Andrade. **Direito e Tecnologia**. Porto Alegre: Livraria do advogado, 2012.

WENDT, Emerson. JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos: Ameacas e procedimentos de investigação**. 2 ed. Rio de Janeiro: Brasport, 2013.