FACULDADE DO ESTADO DO MARANHÃO – FACEM
CURSO DE DIREITO

LUIZ CARLOS COELHO CORREA SEGUNDO

CRIMES CIBERNÉTICOS:

Análise das leis 12.735 e 12.737 no que tange a sua real necessidade de existência.

São Luís – MA
2016

LUIZ CARLOS COELHO CORREA SEGUNDO

CRIMES CIBERNÉTICOS:

Análise das leis 12.735 e 12.737 no que tange a sua real necessidade de existência.

Monografia apresentada a Faculdade do Estado do Maranhão - FACEM, para obtenção do Grau de Bacharel Direito.

Orientador: Prof ºGibson Passinho da Silva.

São Luís - MA
2016

LUIZ CARLOS COELHO CORREA SEGUNDO

CRIMES CIBERNÉTICOS:

Análise das leis 12.735 e 12.737 no que tange a sua real necessidade de existência.

Monografia apresentada a Faculdade do Estado do Maranhão - FACEM, para obtenção do Grau de Bacharel Direito.

Orientador: Prof º Gibson Passinho da Silva.

Aprovado em _____/_____/_____.

BANCA EXAMINADORA

_____

Prof. Esp. Gibson Passinho da Silva
Orientador (a)

_____

Examinador 1

_____

Examinador 2

Dedico este trabalho a Deus pai que tanto iluminou os meus caminhos e os meus pensamentos fazendo com que chegasse até aqui; à minha família, em especial aos meus pais, minha esposa e ao meu filho, Fernando Antônio, que também foram de grande importância nesta minha caminhada.

AGRADECIMENTOS

Agradeço a Deus por ter me dado a graça de estar com saúde e disposição para que eu pudesse galgar mais um degrau em minha vida pessoal e profissional através de um curso superior.

Aos meus pais por terem me orientado na vida de maneira a sempre buscar as coisas boas e fazer o bem aos meus semelhantes.

Ao meu filho e a minha esposa por sempre acreditarem em mim, no meu esforço e no que eu poderia alcançar na vida.

Aos meus amigos e colegas de sala e ao meu grupo de estudos da faculdade que sempre serviu de estímulo para estudar.

“A justiça não consiste em ser neutro entre o certo e o errado, mas em descobrir o certo e sustentá-lo, onde quer que ele se encontre, contra o errado”.

Theodore Roosevelt

RESUMO

Este trabalho tem como objetivo analisar de forma crítica as leis existentes sobre os crimes cibernéticos, no caso as leis 12.735 e 12.737 – Lei Azeredo e Lei Carolina Dieckmann – ambas do ano de 2012, respectivamente, por meio de pesquisas bibliográficas e mostrando a sua real necessidade no mundo jurídico. Em um primeiro momento será abordado o início da internet, como ela surgiu e se expandiu pelo mundo possibilitando um mundo de oportunidades para o "internauta". Para adentrar no aspecto jurídico do tema, foi inserido na pesquisa um breve estudo sobre as velocidades do Direito Penal, seguida de princípios constitucionais que servirão como pontos norteadores ao estudo das referidas leis. Distribuídos em capítulos, os tipos de crimes cibernéticos serão trazidos à tona e por fim a análise das leis as quais já foram citadas juntamente com a sua inutilidade frente às condutas as quais essas se direcionam já tipificadas na legislação penal existente.

Palavras-chaves: Crime Cibernético, leis,

ABSTRACT

This work aims to analyze critically the existing laws on cybercrime, in the case laws 12.735 and 12.737 - Azeredo Law and Carolina Dieckmann Law - both of the year 2012, respectively, through bibliographical research and showing its real Need in the legal world. In a first moment will be approached the beginning of the internet, how it emerged and expanded by the world allowing a world of opportunities for the "internaut". In order to penetrate the legal aspect of the topic, a brief study on the velocities of Criminal Law was inserted in the research, followed by constitutional principles that will serve as guiding points for the study of these laws. Distributed in chapters, the types of cyber crimes will be brought to the fore, and finally the analysis of the laws which have already been cited together with their uselessness towards the conduct to which they are directed, already typified in the existing penal legislation.

Keywords: Cyber Crime, Laws,

LISTA DE SIGLAS

IBGE – Instituto de Geografia e Estatística

ONU – Organização das Nações Unidas

ARPANET – Advanced Research Projects Agency Network

MILNET – Military Network

FTP – File Transfer Protocol

DNS – Domain Name System

NCP – non-player character

TCP – Transmission Control Protocol

WWW – World Wide Web

HTTP – HyperText Transfer Protocol

HTML – Hypertext Markup Language

AOL – America On Line

HOSTS - Hospedeiros

URL – Uniform Ressource Locator

IBM – International Business Machines

PC – Personal Computer

STF – Supremo Tribunal Federal

SUMÁRIO

1 INTRODUÇÃO

Ao longo dos anos o uso da internet vem crescendo vertiginosamente. Estamos vivendo uma verdadeira revolução tecnológica em que nela se contemplam mudanças significativas que influenciam em nosso modo de vida. Os meios de comunicação e as suas formas onde, até então, nunca se cogitavam, surgem de forma bem expressiva e significativa. O mundo digital é repleto de inovações que trazem consigo inúmeras possibilidades de interatividade alcançando uma imensa quantidade de pessoas espalhadas pelo Brasil e no mundo. Nesse pensamento, Telles (2015 apud Martins, 2010) afirma que:

> No presente século, tecnologia é tudo. Em uma casa ou em uma empresa, um computador ou qualquer outro dispositivo informático, eletrônico ou digital, podem ser utilizados para facilitar a consecução de uma variedade de tarefas do dia a dia, tais como administrar contas, estoques, informações de clientes, redigir documentos, fazer cálculos e muito mais; sendo que, para este autor, a essência de qualquer dispositivo tecnológico é o seu *software.*

Porém todo esse avanço trouxe consigo novas possibilidades de se praticar crimes neste ambiente e, dependente como somos deste mundo digital, nos tornamos vulneráveis neste contexto. Os criminosos que detém grande conhecimento em informática, aliado a distancia que o separa de suas vítimas se acabam se beneficiando, concretizando seus crimes. É nesse cenário que as novas práticas criminosas vêm sendo realizadas. Surgem os *cybercrimes.* E com base nesse panorama, cogitou-se a necessidade de se lançar uma lei que fosse específica para estes casos. O presente trabalho visa fazer uma análise quanto aos dispositivos legais existentes que foram sancionados a pouco, em 2012, que são as leis 12.735 e 12.737. Será feita também uma análise de ambos no âmbito constitucional.

Inicialmente será realizada uma abordagem sobre o princípio da internet no mundo, desde o seu uso restrito ao seu período de expansão para o uso comercial, inclusive no Brasil, evolução histórica, as primeiras práticas de crimes mediante o uso de computadores e dispositivos informáticos, tipos de crimes de acordo com a classificação doutrinária e por fim a análise dos referidos diplomas legais bem como os projetos de lei que deram origem a estes e a sua constitucionalidade.

Faz - se necessário destacar que o presente trabalho não esgota toda a matéria relativa aos crimes cibernéticos e leis específicas que os tutelam, mas sim apontam para a real necessidade da lei em epígrafe juntamente com seus efeitos no mundo jurídico.

2 DAS VELOCIDADES DO DIREITO PENAL

2.1 O DIREITO PENAL DE PRIMEIRA VELOCIDADE

O estudo das velocidades do Direito Penal foi criado pelo doutrinador Jésus-Maria Silva Sánchez, onde, segundo ele, o Direito Penal dispõe de três velocidades distintas, onde cada uma delas possuem particularidades na promoção das garantias e das penalidades.

Na primeira velocidade se destaca o Direito Penal tradicional que é definido pela pena de prisão e em virtude disto os diversos princípios constitucionais, serão levados em consideração para a devida aplicação da lei, segundo a afirmação de Rogério Greco[1].

2.2 O DIREITO PENAL DE SEGUNDA VELOCIDADE

O Direito Penal de segunda velocidade conta com certo “abrandamento”, já que caracteriza-se pela não aplicação da pena de reclusão. Houve, na verdade, uma substituição por penas de alternativas podendo ser restritivas de direito, multas, dentre outras. Há uma imposição de obrigações ao indivíduo para reparar o mal causado. Na referida pode haver o afastamento de algumas garantias penais, devido a uma divergência nas inclinações inseridas nesta fase. Um claro exemplo disto é a aplicação da lei dos Juizados, nº 9.099/95, onde são negadas várias garantias como contraditório, ampla defesa e devido processo legal na intenção de tornar mais célere à aplicação da lei.

2.3 O DIREITO PENAL DE TERCEIRA VELOCIDADE

E agora, abordando o Direito Penal de terceira velocidade, destaca-se uma fusão no que tange as peculiaridades existentes nas velocidades anteriores. Trata-se do uso tanto do cárcere como da flexibilização de garantias materiais e processuais. No Brasil já existe uma

[1] GRECO, Rogério. **Direito Penal do Inimigo.** Disponível em: <www.rogeriogreco.com.br/?p=1029> Acesso em: 29 out 2013, p.5.

predisposição desta com a edição das leis nº 8.072, de 1990 (Crimes Hediondos), a Lei nº 9.034, de 1995 (Crime Organizado), dentre outras.

2.4 O DIREITO PENAL DA QUARTA VELOCIDADE

Por fim, a quarta velocidade não tem a sua existência comprovada nos manuais de Direito Penal. Ao que se tem é que essa se fez presente no Tribunal de Nuremberg, quando lá aconteceram julgamentos dos crimes cometidos pelos nazistas no período da Segunda Guerra Mundial. Então, a partir desta premissa, a quarta velocidade do Direito Penal está relacionado ao Direito Internacional. Aqui, a ênfase é dada aos chefes de estado que, ao lançarem a mão dos seus governos ditatoriais, violaram os direitos humanos sendo a eles aplicadas as leis internacionais.

3 PRINCÍPIOS NORTEADORES

3.1 PRINCÍPIO DA LEGALIDADE

Trata-se de um dos princípios mais importantes da Constituição Federal de 1988, pois faz a previsão de que não há infração penal se não houver previsão legal. Leva a crer que tudo o que não for terminantemente proibido, será permitido por lei. É conhecido também pela expressão latina *nullum crimen, nulla poena sine lege*, significando que 'não há crime, nem pena, sem lei anterior que os defina'.

Este princípio nasceu na Inglaterra, e estava previsto na Carta Magna daquele país, no artigo 39:

> **Art. 39.** Nenhum homem livre será detido, nem preso, nem despojado de sua propriedade, de suas liberdades ou livres usos, nem posto fora da lei, nem exilado, nem perturbado de maneira alguma; e não poderemos, nem faremos pôr a mão sobre ele, a não ser em virtude de um juízo legal de seus pares e segundo as leis do País.

De acordo com Rogério Greco[2], o Princípio da Legalidade possui quatro funções fundamentais: a proibição a retroatividade da lei penal; a proibição da criação de crimes e penas pelos costumes; a proibição do emprego de analogia para criação de crimes e para

[2] GRECO, Rogério. **Curso de Direito Penal – Parte Geral**. 18ª ed. Niterói, RJ: Impetus, 2016, p. 96.

fundamentar ou agravar penas e, como quarta função, proibir incriminações vagas e indeterminadas.

O principio em questão bloqueia o recurso à analogia, quando esta venha prejudicar o agente. Então, se o fato não for vislumbrado em lei, não poderá o intérprete, por analogia, tentar por esta forma, abarcar fatos que sejam similares que gere prejuízo daquele.

3.2 PRINCÍPIO DA INTERVENÇÃO MÍNIMA

Este princípio visa a sua aplicação quando houver caso de extrema necessidade, pois essa é a forma de intervenção mais violenta que o Estado possui dentro do campo do particular, se dando esta de forma subsidiária quando os outros ramos do direito não forem suficientes para dirimir questões. O direito penal deve ser usado quando todos os outros dispositivos falharem, sendo este usado como *ultima ratio*, mas sempre respeitando os limites impostos pela Constituição Federal. São consequências do princípio da intervenção mínima o princípio da subsidiariedade e o princípio da fragmentariedade do direito penal.

De acordo com Capez[3], a subsidiariedade como característica do princípio da intervenção mínima, norteia a intervenção em abstrato do Direito Penal. Para intervir, o Direito Penal deve aguardar a "ineficácia" dos demais ramos do direito, isto é, quando os demais ramos mostrarem-se incapazes de aplicar uma sanção à determinada conduta reprovável. É a sua atuação *ultima ratio.*

No princípio da fragmentariedade é estabelecido que o direito penal amparasse um pequeno número de condutas ilícitas fazendo com que os bens jurídicos tutelados sejam abrigados de investidas ações intoleráveis pela sociedade. Assim, sinaliza Cezar Roberto Bitencourt[4]

> O princípio da intervenção mínima, também conhecido como *ultima ratio*, orienta e limita o poder incriminador do Estado, preconizando que a criminalização de uma conduta só se legitima se constituir meio necessário para a prevenção de ataques contra bens jurídicos importantes. Ademais, se outras formas de sanção ou outros meios de controle social revelarem-se suficientes para a tutela desse bem, a sua criminalização é inadequada e não recomendável. Assim, se para o reestabelecimento da ordem jurídica violada forem suficientes medidas civis ou administrativas, são estas as que devem ser empregadas, e não as penais. Por isso, o Direito Penal deve ser a ultima ratio do sistema normativo, isto é, deve atuar somente quando os demais ramos do Direito revelarem-se incapazes de dar a tutela devida a bens relevantes na vida do indivíduo e da própria sociedade.

[3] CAPEZ, Fernando. Curso de Direito Penal I. 16. ed. São Paulo: Editora Saraiva, 2012. 651p.
[4] BITENCOURT, Cezar Roberto. **Tratado de Direito Penal**: Parte geral, I. 19ª ed. rev., ampl. e atual. São Paulo: Saraiva, 2013, p. 54.

Assim, pretende-se exaurir todas as formas de fiscalização além da esfera penal para, enfim, possa ser feito o uso do direito penal para resolver conflitos que surjam na sociedade para que os bens tutelados sejam resguardados.

3.3 PRINCÍPIO DA LESIVIDADE

Este princípio visa a repressão do estado quando o bem jurídico tutelado sofre uma afronta direta. Haja vista que, para que a conduta seja considerada lesiva, é necessário que os interesses de outrem sejam afetados do contrário, as ações praticadas pelo agente fiquem atreladas no âmbito de interesse do mesmo agente.

3.4 PRINCÍPIO DO ESTADO DE INOCÊNCIA

O princípio do Estado de Inocência está previsto no artigo 5º, LVII da Constituição Federal, antecipando "ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória". Cabendo, portanto, ao Estado não apenas promover a investigação, denúncia, processamento e julgamento do acusado, como igualmente, aguardar o trânsito em julgado da condenação para a definitiva imputação da condição de culpado, para efeitos penais e extrapenais[5].

Este princípio possui uma grande relevância, pois, para que o Estado possa efetuar a sua ação persecutória, se faz necessário que o agente, presumidamente, perca a condição de inocente.

3.5 PRINCÍPIO DA LIBERDADE DE EXPRESSÃO

Trazido pela Constituição Federal de 1988, no artigo 5º, inciso IX, e também inserido no artigo 220, §1º, o referido principio destaca a manifestação de pensamento, opinião, atividade intelectual, artística, científica e de comunicação, sem censura. Este princípio desperta para a busca da informação, que por sua vez gera a liberdade de Imprensa, pois alberga o direito de ser informado levando a formar conhecimentos e ideias resultando em um

[5] MUTA, Luiz Carlos Hiroki. **Direito Constitucional**. Tomo I. Rio de Janeiro: Elsevier, 2012.

senso crítico, onde, de acordo com Carlos Roberto Siqueira[6], "um povo desinformado e destituído da capacidade crítica para avaliar o processo social e político acha-se proscritos das condições de cidadania que dão impulso ao destino das nações".

4 DO PRINCÍPIO DA INTERNET AOS CRIMES CIBERNÉTICOS

4.1 BREVE HISTÓRICO DA INTERNET

A internet pode ser considerada nos dias de hoje um marco na Revolução Tecnológica. Milhares de pessoas espalhadas pelo mundo conseguem se ver e se comunicar com um simples toque. De acordo com o IBGE, o número de domicílios conectados correspondem a 54,9% em 2014. Todo esse processo teve início nos anos 60 diante de um cenário de guerra: a Guerra Fria. Desde o lançamento do primeiro satélite O *Sputnik*, pela União Soviética, O Departamento de Defesa Norte Americano deu início à corrida para o desenvolvimento tecnológico, pois queriam sistematizar uma forma de comunicação entre seus diferentes locais destinados à investigação para fins militares. Põe-se em prática a ideia da construção de uma rede que, uma vez criada, teria que apresentar uma grande robustez resistente a um possível ataque que causasse destruição parcial, como por exemplo, de uma explosão nuclear. Daí surge o pesquisador Paul Baran que, à vanguarda deste movimento, desenvolveu todo um conjunto o qual este teria como ponto de partida uma base desconcentrada, ou seja, um local onde pudessem ficar armazenadas todas as informações possíveis e também como elas iriam transitar, já que se tratava de um conjunto que mais tarde se chamaria de rede. Pensou – se, a princípio, em uma grande teia, ou seja, vários pontos ligados uns aos outros para que os dados/informações pudessem trafegar fio a fio e sempre buscando um caminho mais acessível. A ideia do governo americano era descentralizar ao máximo todas as informações distribuindo–as para diversos lugares dando início a uma possível ofensiva nuclear russa, por exemplo, como já foi citado anteriormente.

Ao final dos anos 60 a *Arpanet*, já estava em pleno funcionamento. Ela foi o começo de tudo. Podendo dizer que foi a précursora da Internet no mundo. Criada pela empresa ARPA, no governo do presidente Eisenhower, a Arpanet era uma rede controlada pelos militares. A princípio funcionava interligando centros universitários de Los Angeles, Santa Bárbara, Stanford e Utah.

[6] CASTRO, Carlos Roberto Siqueira *apud Ibidem*, p. 333-334

Logo depois foi desenvolvida uma ferramenta utilizada para emails e com isso as mensagens eletrônicas passaram a ser bastante utilizadas.

Fora criada também a *Milnet* – rede de computadores destinada ao envio de dados das organizações militares – de forma separada já que as universidades trabalhavam para os militares.

No início dos anos 70 a *Arpanet* cresceu em número de computadores conectados e de diferentes plataformas. Constatou-se que era necessário criar uma forma de como os usuários da rede pudessem não só a vir a se conectar de qualquer lugar como também de mover arquivos de um computador para o outro.

Mais tarde esta forma de acesso foi tida como Telenet e a transferência dos arquivos virou *FTP*, que nada mais é do que a transferência e o envio de dados. Para que houvesse o envio e a transferência desses dados foi projetado um protocolo que mais hospedeiros tivessem acesso, além de controlar também o fluxo e o caminho das informações. E que mais tarde daria origem ao *DNS* – servidores de domínio. A velocidade da Arpanet para ligações com linhas telefônicas era de 56 kbps.

Entretanto, ao final da década de 70, a Arpanet desencadeou uma sobrecarga. Nos anos 80 houve o surgimento de outra rede que foi agregada a Arpanet chegando, ao final desta mesma década, aos mais de 100.000 *host*. Destacamos aqui nesse período o lançamento do primeiro PC da IBM mais precisamente em 1981. A empresa que na época tinha a Apple como concorrente usava o sistema operacional da Microsoft, alavancando assim no mercado traçando uma nova linhagem no ramo. Na mesma década, o protocolo *NCP* foi mudado para o *TCP/IP* e que permanece até os dias atuais.

No começo dos anos 90 a internet já toma proporções ainda maiores tanto em expansão como em arquitetura, tendo o seu numero de *host* – maquinas ou computadores conectados a uma rede – ainda maior, podendo oferecer desde informações até serviços e recursos aos usuários da internet. Páginas sem muita dinâmica, conexões discadas e com grandes instabilidades, assim foi marcada a internet já nesta época. Nesta década houve a criação do *World Wide Web* por Tim Berners – Lee, cientista britânico e considerado pai da web. O uso do WWW, colocado antes do endereço de qualquer site que for pesquisado originou-se dessa geração. Tim Berners revolucionou o mundo virtual nesta fase pesquisada apartir da disponibilização da Web para o domínio público já em 1991 quando foi constituído

o primeiro servidor previamente com o *browser*[7]. E não parou por ai. Tim desenvolveu também um sistema de protocolos que atuam na execução da rede mundial, no caso o endereço *URL*, protocolo *HTTP* e o código usado para estruturação das páginas na web – *HTML*.

O grande "boom" da era digital deu-se nesta época. A internet ficou bem popular no mundo com a oferta de vários portais com conteúdos diversos como o *AOL, Yahoo*[8], salas de bate papo e mensageiros como o *ICQ*[9] e o *mIRC*[10], emails gratuitos e as máquinas de buscas que são usadas até os dias de hoje como o *Google* e o *Cadê*, vinculada ao *Yahoo.*

Mas este "boom" ganhou mais robustez nos anos 2000 com o surgimento de mais aplicativos e também das "redes sociais" tais como *Orkut*[11], *My Space*[12], *Twiter*[13], *Facebook*[14] e muitas outras que aproximaram cada vez mais as pessoas, criando um elo ainda mais forte entre milhares de internautas do mundo inteiro.

4.2 CRESCIMENTO DO USO DA INTERNET

Atualmente, vive-se em um mundo digital. Milhares de pessoas vivem conectadas com o mundo e em completa interação. Não se pode negar que quando se reporta à globalização, também se fala no crescimento da internet já que ambos estão ligados diretamente. De acordo com um relatório realizado em 2015 pela rede social *Facebook,* o número de usuários da rede mundial cresceu 200 milhões, totalizando 3,2 bilhões. Se compararmos com 2014 quando uma agencia da ONU publicou que o mundo já possuía quase 3 (três) bilhões de usuários que, em percentuais reais, chegava aos 40% da população mundial. Entretanto, ainda no ano desta última pesquisa, foi constatado que mais de 4 bilhões de habitantes ainda não possuíam o

[7] **Browser** é um programa desenvolvido para permitir a navegação pela web, capaz de processar diversas linguagens, como HTML, ASP, PHP.
[8] **Yahoo! Inc.** é uma empresa norte-americana de serviços de Internet com a missão de ser "o serviço de Internet global mais essencial para consumidores e negócios"
[9] **ICQ** é um programa de comunicação instantânea, o pioneiro dos programas do gênero na internet.
[10] **mIRC** é um cliente de IRC, shareware, para o sistema operacional Microsoft Windows, criado em 1995 e desenvolvido por Khaled Mardam-Bey com a finalidade principal de ser um programa chat utilizando o protocolo IRC, onde é possível conversar com milhões de pessoas de diferentes partes do mundo.
[11] **Orkut** é uma rede social filiada ao Google, criada em 2004 com o objetivo de ajudar seus membros a conhecer pessoas e manter relacionamentos.
[12] **My Space é** uma rede social que utiliza a Internet para comunicação online através de uma rede interativa de fotos, blogs e perfis de usuário.
[13] **Twitter** é uma rede social e servidor para microblogging, que permite aos usuários enviar e receber atualizações pessoais de outros contatos, em textos de até 140 caracteres.
[14] **Facebook** é uma rede social lançada em 4 de fevereiro de 2004, operado e de propriedade privada da Facebook Inc.

acesso a *WEB*[15] e que na África existiam apenas 19% da população que tinha acesso ficando, desta forma, com a menor quantidade de usuários conectados.

Apesar de ter havido um grande aumento no número de conexões feitas no mundo, ainda existem lugares onde esta realidade se encontra um pouco distante, devido a diversos fatores como: falta de infraestrutura em áreas pobres do mundo e longínquas de difícil acesso; o custo do acesso e as habilidades e aceitação cultural necessárias para acessar o serviço de forma prática e simples. Mas para que essa realidade mude será necessária a união de forças entre governo, iniciativa privada e demais entidades para que a inclusão digital seja realizada. Seja coletando dados do atual estágio de conectividade mundial, seja desenvolvendo tecnologias mais disponíveis.

No Brasil este momento é evidenciado constantemente nos últimos anos. Pesquisas demonstram que o aumento do uso da rede mundial vem crescendo com o advento dos *smartphones*[16]. Esses sofisticados aparelhos celular de última geração permitem o acesso direto à internet, emails, redes sociais e inclusive compras virtuais. Desta forma, as possibilidades de ingresso na rede mundial de computadores aumentam, juntamente com o seu público originando um novo cenário a ser explorado para as práticas de crime.

4.3 SURGIMENTO DOS CRIMES VIRTUAIS

Com a evolução da tecnologia o mundo virtual cresce a cada dia. Impossível hoje em dia pensar em mundo sem a internet. São milhares de informações e dados informáticos transitando a todo momento na rede. Isso fez despertar em muitos criminosos uma nova possibilidade, novos espaços a serem tomados para a prática de crimes. Houve uma grande migração desses bandidos com o objetivo de apoderar-se dessas informações para obter vantagem iniciando uma nova categoria de crimes: os crimes cibernéticos.

Não existe um consenso na literatura acerca do surgimento desses crimes. Entretanto existem muitos fatos datados a partir do século XX, nos anos 60. Casos de espionagem eletrônica em sistemas informáticos assim como de sabotagem destes sistemas foram levantados nesse período. Foi desenvolvido por programadores, ainda nessa década, um jogo chamado *Core Wars* que se reproduzia todas as vezes que era ativado causando uma grande sobrecarga na memória do computador do outro jogador. Em contrapartida os mesmos

[15] **Web** é uma palavra inglesa que **significa** teia ou rede.
[16] **smartphone** é um celular com tecnologias avançadas, o que inclui programas executados um sistema operacional, equivalente aos computadores.

mentores desse jogo criaram um dispositivo que era capaz de destruir essas cópias de reprodução originadas do mesmo jogo o que consideraríamos nos dias de hoje como um antivírus.

Podemos fazer destaque também ao surgimento da figura do *hacker* que, na década de 70, já estava em evidência com a invasão feita em sistemas e furtos de softwares em computadores conectados à rede.

Na década de 80 houve uma preocupação maior com as vulnerabilidades que apareceram no sistema, pois foi nesta período que os crimes cibernéticos se alastraram ainda mais, causando grandes problemas e prejuízos para o meio externo. Delitos como invasão de sistemas, pedofilia, pirataria começaram a despertando uma grande preocupação para com comunidade virtual exigindo assim uma postura mais firme no que diz respeito à punição dos responsáveis que podem estar espalhados em diversas partes do globo dificultando, desta forma, a captura do criminoso.

Nos dias atuais, diversos doutrinadores da área possuem um direcionamento relativo a esses atos criminosos, conforme fala Carneiro (2012 apud PINHEIRO, 2006), "O crime virtual é, em princípio, um crime de meio, ou seja, utiliza-se de um meio virtual". Segundo uma pesquisa realizada pela *SaferNet*, uma organização não governamental sem fins lucrativos, que reúne cientistas da computação, professores, pesquisadores e bacharéis em Direito com a missão de defender e promover os Direitos Humanos na Internet, em 2014 os crimes cibernéticos como racismo, xenofobia (forma de discriminação social que consiste na aversão a diferentes culturas e nacionalidades) e tráfico de pessoas cresceram. As denúncias relacionadas a ilícitos praticados na internet aumentaram 8,29% aponta levantamento da Central Nacional de Denúncias de crimes cibernéticos da ONG *SaferNet* Brasil. Foi um total de 189.211 reclamações, envolvendo 58.717 páginas distintas da *web*. A ONG enfatiza que, em virtude da Copa do Mundo no Brasil e as eleições, houve um aumento no número de denúncias relacionadas a práticas de racismo, xenofobia e ao tráfico de pessoas. A divulgação desses dados no Brasil, à época, foram feitas simultaneamente com mais 113 países em referência ao Dia Mundial da Internet.

Os dados apurados mostram ainda um aumento de 34,15% das páginas apontadas como racistas e de 365,46% de conteúdos relacionados à xenofobia. A pesquisa ainda revela que grande parte desses sites fora m criados no período das eleições no intervalo compreendido entre seis de julho e a semana seguinte ao segundo turno. Somente no dia 27 de outubro, foram reportadas à *SaferNet*, 10.376 denúncias anônimas contra

6.909 *links*[17] diferentes nas redes sociais. As declarações de caráter ofensivo contra os nordestinos lideraram nesta época, indicou informou Thiago Tavares, representante da *SaferNet.* Outrossim, houve crescimento de 192,93% nas denúncias envolvendo páginas suspeitas de tráfico de pessoas na comparação com 2013. Constatou-se que "O objetivo era recrutar pessoas, principalmente mulheres, inclusive adolescentes, para a prostituição em cidades-sedes da Copa do Mundo", informou Tavares. As capitais mais citadas foram São Paulo, Rio de Janeiro, Salvador e Fortaleza.

Os casos reportados à *SaferNet* são feitos voluntariamente pelos internautas, quando se deparam com conteúdos que revelem crimes contra os direitos humanos na web. Para realizar a denúncia, o usuário deve acessar o portal da organização através do endereço eletrônico www.safernet.org.br/site/denuciar e enviar o link do site onde se identifica o ato ilícito. (MACIEL, 2015).

5 DOS CRIMES CIBERNÉTICOS

5.1 CONCEITO DE CRIME

A princípio, essa abordagem sobre o referido assunto, não pretende avolumar de forma excessiva a teoria geral do crime, mas mostrar os elementos e a concepção que atualmente vêm sendo aceitas pela doutrina tendo em vista que ainda não há um consenso. Importante destacarmos que, o Código Criminal do Império de 1830 e o primeiro Código Penal Republicano de 1890, traziam consigo o conceito de crime. Diferente da legislação penal atual, onde esta relega à doutrina por meio de diversas colocações espalhadas pelo dispositivo legal. Será feita uma breve análise na qual o crime será visto a partir da concepção formal, material e analítico.

5.1.1 Conceito Formal

Perante o aspecto formal, crime seria toda conduta que atentasse, que fosse de encontro a lei penal editada pelo estado. Considerando-se o seu aspecto material, conceituamos o crime como aquela conduta que viola os bens jurídicos de grande relevância.

[17] **Link** é o "endereço" de um documento (ou um recurso) na web.

5.1.2 Conceito Material

Já o conceito material sobreleva a importância do principio da Intervenção Mínima quando menciona que somente existirá crime quando a conduta do agente atentar contra os bens mais importantes. Porém, mesmo sendo importante e necessário o bem para a manutenção e a subsistência da sociedade, se não houver um dispositivo legal protegendo-o, por mais relevante que seja, não haverá crime se o agente vier atacá-lo, em face do princípio da legalidade.

5.1.3 Conceito Analítico

O Conceito Analítico vem explorar as características ou elementos que formam a infração penal, sem que com isso se queira fragmentá-lo. O crime é, certamente, um todo unitário e indivisível. Ou o agente comete o delito (fato típico, ilícito e culpável), ou o fato por ele praticado será considerado um indiferente penal. O estudo estratificado ou analítico permite, com clareza, verificar a existência ou não da infração. Sobre o conceito analítico do crime, preleciona Assis Toledo:

> "Substancialmente, o crime é um fato humano que lesa ou expõe a perigo bens jurídicos (jurídicos penais) protegidos. Essa definição é, porém, insuficiente para a dogmática penal, que necessita de outra mais analítica, apta a pôr à mostra os aspectos essenciais ou os elementos estruturais do conceito de crime. E dentre várias definições analíticas que têm sido propostas por importantes penalistas, parece-nos mais aceitável que considera as três notas fundamentais do fator crime, a saber: ação típica (tipicidade), ilícita ou antijurídica (ilicitude) e culpável (culpabilidade). O crime, nessa concepção de adotamos, é, pois, ação típica, ilícita e culpável".[18]

De acordo com o que ensina Luiz Regis Prado[19],

> "a ação, como primeiro requisito do delito, só apareceu com Berner (1857), sendo que a ideia de ilicitude, desenvolvida por Ihering (1867) para a área civil, foi introduzida no Direito Penal por obra de Von Liszt e Beling (1881), e a culpabilidade, com origem de Merkel, desenvolveu-se pelos estudos de Binding (1877). Posteriormente, no início do século XX, graças a Beling (1906), surgiu a ideia de tipicidade".

Alguns autores, a exemplo de Assis Toledo e Luiz Regis Prado, aduzem que o crime é composto pela ação típica, ilícita e culpável. Podemos dizer também, sem nos afastarmos

[18] TOLEDO, Francisco de Assis. *Princípios básicos de direito penal,* p.80.
[19] PRADO, Luiz Regis. *Curso de direito penal brasileiro* – Parte geral, p.135

desse conceito, em vez de ação típica, fato típico, pois que, o fato, como veremos no quadro demonstrativo a seguir, abrange a conduta do agente, o resultado dela advindo, bem como nexo de causalidade entre a conduta e o resultado. Portando não vislumbramos diferença que mereça destaque entre as expressões ação típica ou fato típico.

Segue-se quadro demonstrativo, para que possamos visualizar os elementos que compõem a infração penal[20]:

CRIME		
FATO TÍPICO	**ANTIJURÍDICO**	**CULPÁVEL**
- Conduta { dolosa /culposa comissiva/ omissiva - Resultado - Tipicidade { Formal Conglobante	Obs.: quando o agente não atua em: - Estado de necessidade - Legitima defesa - Estrito cumprimento do dever legal - Exercício regular do direito *Quando não houver o consentimento do ofendido como causa supralegal da exclusão da ilicitude	- Imputabilidade - Potencial consciência sobre a ilicitude do fato - Exigibilidade da conduta diversa

5.2 CONCEITO DE CRIME ADOTADO POR DAMÁSIO, DOTTI, MIRABETE E DELMANTO

Damásio,[21] Dotti,[22] Mirabete[23] e Delmanto[24] entendem que o crime, sob o aspecto formal, é um fato típico e antijurídico, sendo que a culpabilidade é um pressuposto para a aplicação da pena. Mesmo considerando a autoridade dos defensores desse conceito, entendemos, *permissa vênia*, que não só a culpabilidade, mas também o fato típico e a antijuridicidade são pressupostos para aplicação da pena. Para chegarmos a essa conclusão, devemos nos fazer as seguintes indagações:

- Se, por alguma razão, não houver o fato típico, poderemos aplicar pena?

Obviamente que a resposta será negativa.

---

[20] GRECO, Rogério. **Curso de Direito Penal – Parte Geral**. 18ª ed. Niterói, RJ: Impetus, 2016, p. 96
[21] JESUS, Damásio E. de. *Direito penal* – p.94
[22] DOTTI, René Ariel. *Curso de direito penal* – Parte geral, p.335-339
[23] MIRABETE, Julio Fabbrini. *Manual de direito penal* – Parte geral, p.94.
[24] DELMANTO, Celso. *Código penal comentado,* p. 18-19.

- Se a conduta do agente não for antijurídica, mas, sim, permitida pelo ordenamento jurídico, poderemos aplicar-lhe uma pena? Mais uma vez a resposta negativa se impõe.

Enfim, todos os elementos que compõe o conceito analítico do crime são pressupostos para a aplicação da pena, e não somente a culpabilidade, como pretendem os mencionados autores.

O fundamento desse raciocínio se deve ao fato de que o Código Penal, quando se refere a culpabilidade, especificamente nos casos em que afasta, utiliza, geralmente expressões ligadas à aplicação da pena, a exemplo do artigo 26, que, cuidando do tema relativo à inimputabilidade, inicia sua redação dizendo que é isento de pena o agente que, por doença mental ou desenvolvimento mental incompleto ou retardado, era, ao tempo da ação ou da omissão, inteiramente incapaz de entender o caráter ilícito do fato ou de determinar-se de acordo com esse entendimento; ou a segunda parte do artigo 21, *caput*, do Código Penal que diz que o erro sobre a ilicitude do fato, se inevitável, isenta de pena.

Vale ressaltar que o Código Penal também utiliza a expressão isento de pena, ou alguma outra com ela parecida, para afastar outras características do crime, ou mesmo apontar causas que impedem a punibilidade do injusto culpável, conforme poderemos verificar pela redação do §1º do artigo 20 do Código Penal, que cuida do chamado erro de tipo permissivo, ou mesmo do artigo 181, que ao prever as escusas absolutórias disse ser isento de pena quem comete qualquer dos crimes previstos no Título II (Dos Crimes contra o Patrimônio), da Parte Especial do Código Penal, em prejuízo: I – do cônjuge, na constância da sociedade conjugal; II – de ascendente ou descendente, seja o parentesco legítimo ou com causas que eliminam a culpabilidade, uma vez que, o fato praticado pelas pessoas por ele elencadas é típico, ilícito e culpável. Somente por questões de política criminal é que a lei entendeu por bem não puni-los.Assim, embora o Código Penal utilize essas expressões quando quer se referir às causas dirimentes da culpabilidade, tal opção legislativa não nos permite concluir que o crime seja tão somente um fato típico e antijurídico.

Estamos com a maioria da doutrina, nacional e estrangeira, que adota a divisão tripartida do conceito analítico, incluindo a culpabilidade com um de seus elementos característicos[25].

[25] GRECO, Rogério. **Curso de Direito Penal: Parte Geral.** 14ª Niterói, RJ: Impetus, p. 139 –

5.3 CONCEITO E CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS

A tecnologia sofreu um avanço significativo com o advento da internet. A expansão é notória quando observamos que os meios de comunicação ficaram mais evoluídos e acessíveis a um percentual maior da população. Comprar, conversar com os amigos e até mesmo namoros vem acontecendo pela rede. Hoje em dia é absolutamente normal e possível. A internet veio pra ficar, mas diante de toda essa facilidade, os crimes nesse cenário tomaram forma mais sutil e estão se tornando bastante corriqueiro, crescendo a cada dia, fazendo mais vítimas e transformando o ambiente virtual um local perigoso e repleto de armadilhas. Para os crimes desta categoria, em virtude de ser um lado novo também no mundo jurídico, não existe uma nomenclatura correta. Desta forma esses delitos são denominados também de Crimes Virtuais, Crimes Digitais, Crimes Computacionais dentre vários outros tipos. Para que haja um melhor entendimento, se faz necessário compreendermos o conceito de crime sob a égide do Código Penal Brasileiro. De acordo com Lima Carvalho (2014 apud CAPEZ, 2008):

> [...] material, como "todo fato humano que, propositada ou descuidadamente, lesa ou expõe a perigo bens jurídicos considerados fundamentais para a existência da coletividade da paz social". E, formal, onde o "crime resulta da mera subsunção da conduta ao tipo legal e, portanto, considera-se infração penal tudo aquilo que o legislador descrever como tal, pouco importando o seu conteúdo".

Já no conceito analítico, o crime informático, que também é uma espécie de delito cibernético é "toda ação típica, antijurídica e culpável, cometida contra ou pela utilização do processamento automático de dados ou transmissão". (VELLOSO, 2015 apud Ferreira, 2000, p. 210).

E já partindo dos conceitos acima citados sobre crime, Da Silva (2014, p 34), relata que:

> Importante destacar, que os crimes cometidos em meio ambiente virtual ou contra os dados e sistemas de funcionamento de uma máquina informatizada, são consequência da evolução dos equipamentos de comunicação eletrônicos/informatizados e da internet.

Conforme já fora dito anteriormente, grande parte dos doutrinadores não possui um consenso no que tange este instituto, entretanto existe também uma classificação bem evidenciada nas literaturas atuais. Seguindo o que diz Velloso (2015 apud Corrêa, 2000b, p. 43), os crimes cibernéticos, são "todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou

fraudar”. É importante destacar que, de acordo com o que foi colocado no parágrafo anterior, o ato delituoso seria contra a máquina, o computador em si, ou seja, crimes cometidos contra os dados existentes no dispositivo. Destruição de softweare e dados, furto de informações dentre outros são exemplos de alguns danos que o seu PC pode vir a sofrer. Então, para classificarmos de forma mais instrutiva, a classificação mais aceita pela doutrina é a divisão entre crimes cibernéticos Puros e Impuros ou Mistos.

5.3.1 Crimes cibernéticos puros:

Os Crimes Cibernéticos Puros são aqueles em que o agente necessita imprescindivelmente do computador para realizar ataques remota ou diretamente com uso de sistemas informáticos todo o bem jurídico já tutelado. Nesta situação estão envolvidas não só a invasão e captura dos dados salvos em massa, mas também a intenção de alterar, inserir, adulterar ou destruir dados existentes no computador. Nesta linha de pensamento, Carneiro (2012 apud Viana, 2003, p. 13-26), diz que “São aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados).” Ainda nesse contexto, Carneiro (2012 apud Damásio, 2003) se posicionam da seguinte forma:

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

Destacamos também a presença de duas figuras nesta mesma conjuntura: Os *hackers* e os *crackers.* Segundo a pesquisa ao dicionário Michaelis, um dos significados do termo hacker é: “pessoa que usa seu conhecimento técnico para ganhar acesso a sistemas privados”. Fazendo uma análise sobre a acepção desta palavra, podemos concluir que esta é a pessoa que detém um conhecimento singular acerca do assunto e que não necessariamente o use com o propósito de atuar na ilegalidade porque a partir desse discernimento conclui-se que o domínio no referido assunto pode ser visto de forma positiva e negativa. Já os crackers são pessoas que agem focando a vantagem ilícita. Eles invadem e destroem sites, sejam eles quais forem, fazem quebra de senhas, desenvolvem softwares capazes destruir várias máquinas ao mesmo tempo.

5.3.2 Crimes cibernéticos impuros

Os crimes cibernéticos impuros ou impróprios são aqueles que são praticados com o uso do computador. Diferente dos crimes cibernéticos Puros, esta forma de delito usa o computador como um mero instrumento para a realização deste. Entretanto, os crimes que são realizados com este “auxílio” já são tipificados pelo Código Penal Brasileiro demonstrando que o uso do PC não é um fator primordial mais sim uma das diversas formas de materializar uma conduta delituosa que já está tutelada. Desta forma, Carneiro (2012, apud Damásio, 2003) demonstra:

> [....] Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não-computacionais ou diversos da informática.

Tendo como base essa distribuição se torna mais acessível e mais compreensível o entendimento sobre o que vem a ser os crimes cibernéticos Puros e os Impuros, enfatizando sempre que um necessariamente precisa do computador, vez que a outra modalidade precisará do PC apenas como instrumento para a realização do delito.

6 DA APROVAÇÃO DAS LEIS 12.735 E 12.737 AMBAS DE 2012

Os referidos diplomas legais oriundos dos projetos de lei 84/1999 e 2793/2011, destinados a reprimir os crimes cibernéticos no Brasil, alcançou, a princípio, um grande destaque. Visto que novas tecnologias surgiram no intuito de aprimorar os meios de comunicação, as novas leis regulariam os recentes hábitos fazendo com que este mundo virtual não ficasse desprovido da tutela jurídica do Estado. Entretanto, após análises de vários doutrinadores, percebeu-se que este movimento resultou mais uma das leis sem funcionalidade direta para com o objetivo o qual foi editada. Neste ponto é necessário destacar que, com o Código Penal existente, os crimes praticados neste âmbito, poderiam ser com este combatido. Para que houvesse uma “sintonia” para com essa geração virtual, a legislação penal já existente teria que sofrer uma grande atualização aos moldes dessa linhagem fazendo com que os delitos executados nesse novo ambiente não fugissem ao controle do Estado. Não há dúvidas de que com a evolução tecnológica, que cresce a passos longos, houvesse um incremento nas práticas criminosas.

Neste viés, Telles (2015, Apud GRECO 2012) afirma que:

> O século XXI está experimentando um avanço tecnológico inacreditável. Situações que, no passado, eram representadas em filmes e desenhos infantis como sendo prospecções futuristas, hoje são realidade. As conversas online, em que as visualizações de imagens dos interlocutores, seja por meio de computadores ou *smartphones*, são instantâneas. O mundo está, definitivamente, globalizado e interconectado.

Desse modo, é evidente que o direito caminha de mãos dadas frente à evolução da sociedade, ou seja, deu-se o fato vem o direito logo em seguida para regular.

6.1 DO PROJETO Nº 84/99 À EDIÇÃO DA LEI Nº 12.735 (LEI AZEREDO)

Este projeto de lei nasceu em 1999, apresentado pelo então deputado Luiz Piauhylino, falava acerca da punição dos crimes praticados no meio virtual. Desde então, este projeto foi discutido por mais de dez anos em Brasília. A cronologia deste fato começa com a aprovação na Câmara dos Deputados quatro anos depois. Apensados a esse projeto, por questões de identidade e natureza da matéria, existiram outros dois: PL 76 e 137 ambos do ano de 2003. Seguindo para o senado, o projeto tramitou até o ano de 2008. Ficou conhecido como a Lei Azeredo porque teve este como seu relator tanto na câmara como senado.

Para que este projeto fosse aprovado houve uma redução drástica sobrando da redação original apenas seis dos vinte e três artigos e quando da sanção presidencial, ainda dois artigos foram vetados pela então presidenta Dilma Rousseff, resistindo apenas quatro, *in verbis:*

> **LEI Nº 12.735, DE 30 DE NOVEMBRO DE 2012.**
> **A PRESIDENTA DA REPÚBLICA** Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:
> Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.
> Art. 1º Esta Lei altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.
> Art. 2º (VETADO)
> Art. 3º (VETADO)
> 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.

> Art. 5º O inciso II do § 3º do art. 20 da Lei nº 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação:
> "Art. 20. .....
>
> § 3º .....
>
> II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio;
> ....." (NR)
> Art. 6º Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.
> Brasília, 30 de novembro de 2012; 191º da Independência e 124º da República.
> DILMA ROUSSEFF
> *José Eduardo Cardozo*
> *Paulo Bernardo Silva*
> *Maria do Rosário Nunes*
> Este texto não substitui o publicado no DOU de 3.12.2012

.

Ainda na fase de projeto, a lei recebeu o apelido de AI – 5 digital porque existiam pontos polêmicos, pois violavam direitos fundamentais dos clientes da internet.

Com os vetos e ainda com a retirada dos demais artigos, a lei tornou-se vazia e delicada quanto à sua eficácia. A redação aprovada define que os órgãos da polícia judiciária deverão criar delegacias especializadas no combate a crimes digitais (art. 4º). Essa cautela é bem aceita. Entretanto, isto dependerá muito do Estado para prover toda essa estrutura que cerca este dispositivo que vai desde a especialização dos policiais até a aquisição e a modernização do aparato das forças policiais.

6.2 DO PROJETO DE Nº 2793/11 À EDIÇÃO DE LEI Nº 12.737 (LEI CAROLINA DIECKMAN)

O projeto supracitado, de autoria do deputado Paulo Teixeira (PT/SP), que tipifica crimes cibernéticos, foi aprovado simbolicamente em maio de 2012. A princípio o projeto foi visto como uma saída viável para a ausência de um instituto próprio para os crimes cibernéticos. Contudo, o projeto elencava um rol de tipificações penais escasso pois não abordava pontos bastante discutíveis como a pornografia infantil, a guarda dos logs[26] de acesso pelos usuários da internet, preservação dos direitos autorais, dentre outros. Um dos indícios para que todo esse escopo jurídico fosse sancionado, foi o badalado caso Carolina Dieckmann, atriz famosa, que teve fotos íntimas furtadas do seu computador e divulgadas na rede após ser também chantageada e ameaçada. Desde então houve uma verdadeira comoção

[26] **LOGS** – registro de eventos em um sistema de computadores.

diante do fato. O apelo midiático estava lançado. Com isso, a tramitação ocorreu de forma rápida e o projeto foi despachado em 06 (seis) de novembro de 2012 pelas Comissões de Segurança Pública e Combate ao Crime Organizado e Constituição e Justiça e de Cidadania, transformando-se na Lei Ordinária nº 12.737, publicada no Diário Oficial no dia 03 (três) de dezembro de 2012, pela Presidenta da República, Dilma Russeff, entrando em vigor após a Vacatio Legis de 120 dias, *in verbis:*

LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.

Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.

A PRESIDENTA DA REPÚBLICA, Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.

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.

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no **caput**.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."

"Ação penal

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se 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."

Art. 3º Os arts. 266 e 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação:

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

> Art. 266. .....
> § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
> § 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.” (NR)
> **“Falsificação de documento particular**
> Art. 298. .....
> **Falsificação de cartão**
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.” (NR)
> Art. 4º Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.
> Brasília, 30 de novembro de 2012; 191º da Independência e 124º da República.
> DILMA ROUSSEFF
> *José Eduardo Cardozo*
> Este texto não substitui o publicado no DOU de 3.12.2012

6.3 DA INCONSTITUCIONALIDADE DA LEI 12.735 DE 2012

Conforme já foi mencionado nos tópicos anteriores, o projeto que deu origem à lei nº 12.735 de 2012, foi debatido por vários anos no Congresso Nacional. Objeto de muitas discussões e polêmicas, pois criminalizava de uma maneira bem generalizada, tipificando até conduta culposa, algo totalmente diverso do que está inserido na Convenção de Budapeste, da qual o Brasil ainda não é signatário.

Na prática dessa conduta culposa, o cidadão que encaminhasse, desprovido de qualquer conhecimento, e-mails, contendo arquivos maliciosos, seria considerado crime sendo este punido “inocentemente” com pena privativa de liberdade variando de três a cinco anos. No Instituto Penal nº 12.735, é clara a violação aos princípios constitucionais que são o da Liberdade de Expressão e do Estado de Inocência. A evidência se mostra quando o referido instituto alterou a lei nº 7.716/1989, a Lei de Crimes Raciais, admitindo que o juiz ordene a paralisação das transmissões de símbolos ou similares com o propósito de difundir a discriminação ou o preconceito. No artigo 5º, inciso LVII, da nossa Carta Magna traz, *in verbis*:

> **Art. 5º** Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> **LVII** - ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória.

Neste caso, o Estado terá que originar todo o processo investigatório, a denúncia e o julgamento do acusado, assim como aguardar o trânsito em julgado da sentença, em fase definitiva, para nesse momento ser a ele imputado à condição de culpado para efeitos penais e extrapenais, caso contrário o Princípio do Estado de Inocência estará sendo vilipendiado ao passo em que se permite que o juiz condene o suposto criminoso sem sequer haver o procedimento investigatório, tal como o Princípio da Ampla Defesa e do Contraditório, inciso LV, *in verbis:*

> LV - aos litigantes, em processo judicial ou administrativo, e aos acusados em geral são assegurados o contraditório e ampla defesa, com os meios e recursos a ela inerentes;

O Princípio da Inocência possui um elo com o Princípio da Ampla Defesa e do Contraditório, vez que a parte contrária deverá se pronunciar sobre tudo o que foi lançado em juízo. outrossim, com a proteção do principio da liberdade de expressão, verifica-se que o usuário que tiver qualquer publicação interrompida sem a comprovação de que realmente está infringindo um bem juridicamente tutelado, terá cerceado o seu direito de expressão. Ora, vivemos em um país onde, de acordo com a nossa Carta Magna, a democracia é uma característica muito forte nos remetendo ao sentimento de liberdade e também o da igualdade para que nos deleitemos em direitos e oportunidades. O gozo deste direito a informação se faz necessário na construção de um senso crítico do indivíduo, colaborando assim na produção da personalidade deste. Sem a informação a evolução da personalidade se tornará algo inerte.

As inovações tecnológicas trazidas com o advento da internet facilitam não só a vida do indivíduo, como também agrega as bases para uma reflexão propositiva e diálogos argumentativos, potencializa o processo de disseminação das informações fomentando assim a busca por conhecimento.

6.4 O PROJETO SOPA E PIPA FACE À LEI 12.735/2012 (LEI AZEREDO)

Os projetos *Stop Online Piracy Act (*Pare com a pirataria online) e o *PROTECT IP Act* (ato para a proteção da propriedade intelectual), conhecidos como SOPA e PIPA, respectivamente, diz respeito aos projetos de lei apresentados ao senado americano com o objetivo de bloquear sites e ferramentas de busca da internet que atentem contra a propriedade intelectual dos estadunidenses. Contudo, isso poderia gerar uma grande censura eletrônica em pleno século XXI, prejudicando o livre compartilhamento existente na

internet. Na época, sites que possuem grande relevância tais como *Google*[27], *Wikipédia*[28], *Craiglist*[29], *Facebook,* dentre outros, provocaram grandes manifestações. Alguns até chegaram a retirar suas páginas do ar. Um verdadeiro *blackout*[30] foi promovido como forma de alertar os internautas sobre o que estaria por vir. O site de compartilhamentos de arquivos *Megaupload*[31] foi fechado, e o seu fundador Kim Schmitz, foi preso juntamente com outros três executivos da empresa. A indústria do *copyright*[32] era uma das maiores interessadas na aprovação de tal projeto visto que, com isso, não teriam suas séries, filmes, animes, todo e qualquer arquivo pirateado. Era uma tentativa de combate à violação aos direitos autorais e o tráfico on-line de produtos falsificados.

Se este projeto fosse sancionado pelo presidente, qualquer site que possuísse link com outro suspeito de praticar pirataria, poderia ser retirado do ar a pedido do governo norte americano ou dos produtores do conteúdo. Para quem compartilhasse conteúdo pirata por dez ou mais vezes ao longo de seis meses, a proposta do SOPA era ter penas de até cinco anos de prisão para os apenados que compartilhar. Neste caso, sites como *Google ou o Facebook,* também poderiam ser condenados por permitirem ou facilitarem a pirataria na internet, tendo como pena o encerramento dos serviços e banimento dos provedores de internet, juntamente com os sistemas de pagamento e anunciantes em nível internacional.

As referidas propostas geraram grandes discussões acerca do assunto, sendo também alvo de inúmeras críticas já que isso representava a instauração de uma grande censura e afetaria diretamente a liberdade de expressão bem como a livre circulação de ideias. Na Ásia, mais precisamente em países ditatoriais como a China e a Coréia do Norte, já existe um modelo aos moldes do SOPA. E na Europa, a Lei Sinde, na Espanha e a Hadopi, na França, já são uma realidade. A lei Hadope determina que os provedores desconectem o usuário que esteja fazendo o compartilhamento de arquivos sem a devida autorização e já tenha violado por três vezes. Já a Sinde, autoriza que o governo aja contra os provedores de acesso. Na realidade, ambas vão de encontro aos direitos civis dos internautas.

---

[27] **Google** é uma empresa multinacional americana de serviços online e software.
[28] **Wikipédia** é uma enciclopédia *on-line* e, como um meio para esse fim, é também uma comunidade virtual formada por pessoas interessadas na construção de uma enciclopédia de alta qualidade, num espírito de respeito mútuo.
[29] **Craigslist** é uma rede de comunidades online centralizadas que disponibiliza anúncios gratuitos aos usuários.
[30] **Blackout -** apagão
[31] **Megaupload** foi um serviço multilíngua de download e upload de arquivos.
[32] ***Copyright*** é um direito autoral**,** a propriedade literária, que concede ao autor de trabalhos originais direitos exclusivos de exploração de uma obra artística, literária ou científica, proibindo a reprodução por qualquer meio.

Por fim, após as diversas críticas e manifestos, os projetos supradiscutidos, referidos foram arquivados. Porém, nada obsta que possam surgir novas leis, com a mesma finalidade, para serem debatidos novamente.

6.5 DA ANÁLISE BEM COMO DA DESNECESSIDADE DA LEI 12.737 DE 2012

O referido diploma legal foi aprovado em dezembro de 2012 entrando em vigor no ano seguinte, adicionando Código Penal Brasileiro (Decreto-Lei 2.848 de 7 de dezembro de 1940) os artigos 154-A, 154-B e modificando os artigos 266 e 298 do mencionado código.

A Lei Ordinária nº 12.737/2012 foi apelidada de Lei Carolina Dieckmann. Tal cognome se deu em razão da atriz global, Carolina Dieckmann, ter os arquivos pessoais subtraídos do seu computador assim como as suas fotos em situações intimas publicadas na internet. A imprensa, com o seu grande poder de alcance e persuasão, provocou um grande apelo midiático fazendo com que a tramitação do projeto de lei já citado em outro capítulo fosse realizada em um prazo recorde no Congresso Nacional, passando a frente de outras propostas que já esperavam a mais tempo para entrar em pauta.

A lei trouxe em seu bojo a tentativa de tipificar os crimes de criação e propagação de vírus de computador, a invasão de sistemas, dentre outros. O dispositivo legal inseriu no Código Penal os artigos 154-A e 154-B, originando a invasão de dispositivo informático bem como a normatização da ação penal respectivamente, onde esta última se procederá mediante representação, exceto se a ação criminosa for cometida contra a Administração Pública, pois essa se dará incondicionalmente.

O artigo 154-A, em seu caput, traz o termo “invadir” quando o agente:

> “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, instalar vulnerabilidades ou obter vantagem ilícita”.

O referido termo remete a mecanismos de segurança existentes na máquina podendo ser senhas, *firewalls*, filtros *antispam*, filtros *antiphishing*, dentre outros. Neste aspecto a lei deixa claro que o acesso indevido deve ter como objetivo fim a alteração ou destruição de dados informações que devem ser preservadas. Desta forma, caso o dispositivo se encontre desprotegido, haverá o entendimento de crime impossível por impropriedade absoluta do objeto quando uma dessas “barreiras” forem ultrapassadas o crime houver se consumado. É

fundamental que tenhamos a noção sobre o que pode ser considerado dispositivo móvel, uma vez que, não se se restringe somente a computadores como também aos telefones celulares, os *smartphones*, *tablets*, dentre outros.

Ainda sobre o artigo 154-A, se faz necessário destacarmos também que a sua redação denota uma certa redundância. No caput o termo "invadir" preconiza que o dispositivo informático, alvo do crime, seja acessado indevidamente através da quebra dos mecanismos de segurança, podendo ser a ruptura da senha. Indo mais adiante na redação esta traz consigo a expressão "sem autorização expressa ou tácita do titular do dispositivo". Ora, observemos que sem a devida autorização não há o que se falar em invasão. Tendo em vista que o explorado verbete já revela tal pensamento.

Destaca-se ademais que, caso a violação do dispositivo informático aconteça, mas com o intuito apenas de observar o conteúdo existente na máquina, não ilustrará a conduta criminosa. Entretanto, do ponto de vista da proteção ao bem jurídico o qual se pretendia guardar, nesse caso os dados, foi maculado.

No que tange as penas acerca desse crime, as condutas explanadas aqui, possuem um tempo não superior aos dois anos, transformando, assim em delitos de menor potencial ofensivo abrangidos pela lei 9.099/1995, artigo 61, *in verbis:*

> Art. 61. Consideram-se infrações penais de menor potencial ofensivo, para os efeitos desta Lei, as contravenções penais e os crimes a que a lei comine pena máxima não superior a 2 (dois) anos, cumulada ou não com multa.

Isto significa que o feito será julgado no âmbito dos Juizados Especiais Criminais. Contudo, isso não se torna regra porque grande parte dos processos gerados impunham um certo grau de complexidade, tendo em vista a concretude dessa infração que quase sempre serão provadas por meio de perícias técnicas, este será remetido ao juízo comum contemplando agora o artigo 156 do Novo Código de Processo Civíl, *in verbis:* O juiz será assistido por perito quando a prova do fato depender de conhecimento técnico ou científico.

Já a análise do artigo 154-A, §1º, traz consigo a criminalização daqueles que fabricam, oferecem, distribuem ou vendem a terceiros, ou simplesmente divulgam aleatoriamente dispositivos ou programas de computador que podem ser utilizados por terceiros para acessarem indevidamente dispositivos informáticos ou impor condições de risco. Sobre estas condições de risco que são "instaladas", existe uma inadequação no uso de termos técnicos na letra da lei. A vulnerabilidade, provocada pela condição de risco, não será instalada e sim

explorada a partir do simples clique no arquivo malicioso em que a partir deste instante tal arquivo será inserido. Isso ocorre quando um email chega ao destinatário trazendo consigo um anexo e nele contenha um vírus que, se acessado, poderá introduzir-se no PC. Doravante com o vírus já instalado na máquina o criminoso poderá realizar a captação de todos os dados pessoais existentes como as senhas de tudo o que é acessado no referido equipamento.

O parágrafo 2º (segundo) do artigo 154-A incluiu o aumento da pena de um sexto a um terço caso resulte prejuízo econômico, seguida do parágrafo 3º (terceiro) que majorará, também, a obtenção das informações mais reservadas armazenadas na máquina da vítima.

A redação do parágrafo 3º (terceiro) trouxe penas mais enérgicas nos casos em que houver "obtenção de conteúdos privados, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido". Se faz necessário destacar que a manutenção realizada de forma remota do sistema dos usuários de serviços telemáticos não configura crime, ressalvado quando esta transcender os limites quanto ao objetivo fim daquele acesso e que resulte em adulteração ou destruição de dados ou informações.

Trazendo à tona o parágrafo 4º, que traz a causa de aumento de pena de um a dois terços sempre que houver "divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos, se o fato não constitui crime mais grave", este discorre sobre uma precisão de um esclarecimento em relação ao parágrafo anterior porque intrinsecamente a obtenção de informações sigilosas e de segredos comerciais ou industriais já possui o objetivo de auferir lucro/ vantagem para o criminoso ou, até mesmo, um grande prejuízo ao seu oponente, gerado pela conjectura da divulgação indevida para o mercado. A publicação desses dados podem ir ao encontro o artigo 195, inciso XII, da Lei 9.279/1996, configurando o crime de concorrência desleal. Entretanto, em virtude da Lei 12.737/12 ter sido sancionada subsequentemente àquela, sustenta-se que se predominará na categoria "divulgação" e "exploração".

Encerrando com o parágrafo 5º, ainda em relação ao artigo 154-A, a pena terá um incremento de um terço até a metade se a conduta for praticada contra quaisquer das autoridades elencadas no referido artigo. Partindo para a ação penal, no caso desse crime ser praticado contra alguma daquelas pessoas citadas no parágrafo 5º, do artigo 154-A, esta se dará independente de representação.

O diploma legal 12.737 de 2012, alterou da mesma forma os artigos 266 e 298 do Código Penal, objetivando proteger a constante disponibilidade dos serviços de comunicação

e informação e utilidade pública. Do parágrafo 1º, do mesmo artigo, que traz a expressão jurídica ”quem” interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento, pretendeu-se tipificar a conduta de quem realiza ataques de negação de serviços. Tal ação é chamada de *Denial of Service*[33], que consiste em transformar os recursos em status de indisponível para os usuários da internet, ou seja, as páginas da *“web”* se tornarão inacessíveis. É necessário mencionar quanto à violação deste preceito que ocorrerá quando tão somente o serviço afetado seja público, ainda que este seja explorado por empresas privadas que detenham concessão, permissão ou autorização expedida pela Anatel. Desta forma conclui-se que, quem pratica atividade privada de cunho econômica, através do comércio eletrônico, e que não seja de utilidade pública, não estará abrigado neste arcabouço jurídico.

Finalmente, temos o artigo 298 que trata sobre crimes de falsificação, também foi alterado, equiparando agora cartão de crédito e débito a documento particular. Relembramos que a redação do Código Penal já trazia em seu bojo tal tipificação, pois a conduta recai sempre sobre a obtenção de vantagem ilícita em prejuízo alheio. Assim, esta prática delituosa já é contemplada pelo crime de estelionato e nos termos da Súmula 17 do Supremo Tribunal Federal que dispõe da seguinte forma: “QUANDO O FALSO SE EXAURE NO ESTELIONATO, SEM MAIS POTENCIALIDADE LESIVA, E POR ESTE ABSORVIDO”. Caso o agente confeccione cartões sem atribuir nenhuma numeração, será punido pelo crime em si, tornando-se incomum devido ao fato de que as adulterações não se efetuam tão somente com a produção indevida dos cartões mas sim com a inserção dos números. Seguem abaixo algumas jurisprudências que antecederam a lei 12.737/2012:

> PENAL. PROCESSO PENAL. CONFLITO DE JURISDIÇÃO. INQUÉRITO POLICIAL. FRAUDE BANCÁRIA. CAIXA ECONÔMICA FEDERAL. TRANSFERÊNCIA DE VALORES POR MEIO ELETRÔNICO (INTERNET). FURTO MEDIANTE FRAUDE. (ART. 155, § 4º, INC. II, CP). FORO DA CONSUMAÇÃO DO DELITO. LUGAR ONDE SITUADA A AGÊNCIA EM QUE MANTIDA A CONTA-CORRENTE LESADA. PRECEDENTES (STJ E TRF4).
> 1. Consolidou-se o entendimento de que a subtração de valores de conta-corrente ou conta-poupança - sem a autorização do titular e por meio de expediente eletrônico fraudulento (Internet) - configura o crime de furto mediante fraude (art. 155, § 4º, inc. II, CP).
> 2. Considerando que o delito de furto se consuma no momento em que a coisa móvel é retirada da esfera de disponibilidade da vítima e colocada em poder do agente, competente para apreciar o feito é o juízo do lugar onde situada a agência da CEF em que mantida a conta corrente lesada.
> 3. Precedentes do Superior Tribunal de Justiça e deste Tribunal.

[33] **Denial of Service** é uma tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores

> FURTO QUALIFICADO - AUTORIA DELITIVA
> PROVADA - RECURSO PROVIDO. Suficientes os elementos probatórios a demonstrar a autoria de agente que subtraiu coisa alheia móvel, mediante fraude realizada por meio da internet, de rigor o decreto condenatório.
> FURTO QUALIFICADO - REGIME CARCERÁRIO MAIS GRAVOSO - CONVENIÊNCIA DE REGIME INICIAL FECHADO. Pode o Juiz impor regime prisional inicialmente fechado, independente do montante da privativa de liberdade e a primariedade do réu, em observância com as circunstâncias presentes no fato delituoso, em conjunto com aquelas previstas no artigo 59, do Código Penal.
>
> PENAL E PROCESSUAL PENAL. FRAUDE NA REDE MUNDIAL DE COMPUTADORES (INTERNET). ART. 171, § 3º, DO CP. COMPETÊNCIA DO LUGAR ONDE O AGENTE COMETE O DELITO.
> I - No caso concreto, não há que se falar no delito de furto, caracterizado pela subtração, mas sim em crime de estelionato qualificado (art. 171, § 3º, do CP), já que o fato investigado - utilização de meio fraudulento para sacar dinheiro de correntistas da Caixa Econômica Federal -, leva, em tese, à configuração deste último.
> II - Tratando-se de crime de estelionato, a competência para processálo e julgá-lo é do lugar em que o agente efetivamente obteve a vantagem indevida, ou seja, onde ocorreu o dano. Precedentes.
> III - Recurso desprovido.
> "Crime de Computador": publicação de cena de sexo infanto-juvenil (E.C.A., art. 241), mediante inserção em rede BBS/Internet de computadores, atribuída a menores: tipicidade: prova pericial necessária à demonstração da autoria: HC deferido em parte.
> 1. O tipo cogitado - na modalidade de "publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente" - ao contrário do que sucede, por exemplo, aos da Lei de Imprensa, no tocante ao processo da publicação incriminada é uma norma aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador.
> 2. Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta criminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo.
> 3. Se a solução da controvérsia de fato sobre a autoria da inserção incriminada pende de informações técnicas de telemática que ainda pairam acima do conhecimento do homem comum, impõe-se a realização de prova pericial.

O Supremo Tribunal Federal, nos diversos julgamentos apresentados acima e em atenção ao ultimo mencionado, em que declara: “a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo”, manifesta claramente que faz uso da interpretação extensiva e que tem como característica principal a carência da lei em relação à abrangência, ou seja, amplia o sentido da norma já que esta vem dizendo bem menos do que deveria. Desta forma, o STF manifesta que, o direito deva estar em perfeita harmonia com

as mudanças que ocorrem no meio social, para que dessa forma, possa ser interpretado demonstrando a pretensão da lei: a tutela dos bens jurídicos.

6.6 DA ANÁLISE DOUTRINÁRIA EM RELAÇÃO À LEI 12.737/2012

Quanto a lei em epígrafe, os doutrinadores são categóricos em falar que os crimes cibernéticos dispensam a edição de leis com o intuito de regular tal ilícito. Além do que, será necessário que haja uma completa reestruturação nas delegacias, inclusive treinamento do efetivo de policiais, pois esta situação gera uma grande discussão acerca do assunto. Não é salutar que se adicione um tipo penal de violação de dispositivos informáticos, se a policia não estiver preparada para investigar e instruir devidamente o inquérito sobre tais crimes (VIANA 2013). Salienta-se ainda que cabe aos operadores do direito lançar a mão da interpretação de determinadas condutas em face a legislação penal existente, uma vez que esta se encontra tipificada, faltando apenas amoldar aos velhos tipos penais com a sua correta e atualizada interpretação jurisprudencial (VIANA 2013). Diferenciam-se os crimes que são praticados com o uso da o computador e os que são realizados contra o sistema do computador. Exemplifica bem essa separação com o crime de ameaça, que, de acordo com ele, antigamente se escrevia um bilhete, entretanto, esse mesmo crime pode acontece hoje por e-mail ou recado deixado num site de relacionamento. Trata-se do mesmo crime, todavia, a tecnologia serviu como uma ferramenta para praticá-lo. A ameaça praticada por meio de um bilhete é a mesma feita no âmbito virtual. A mudança trazida pelo artigo 147 do Código Penal foi a forma como o crime foi praticado. Agora, quando o alvo, o objetivo do criminoso é o sistema informatizado, como a supressão de seus dados, está-se diante de outro cenário (VIANA 2013).

> **Ameaça**
> Art. 147 - Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave:
> Pena - detenção, de um a seis meses, ou multa.
> Parágrafo único - Somente se procede mediante representação.

A fraude realizada nos bancos é outro exemplo bem claro e corriqueiro. É um crime que também poder ser praticado por meio eletrônico. Outrora falsificava-se cheques e dados cadastrais e atualmente esse ato é realizado com apenas um clique no *mouse*. É o conhecido Cavalo de Tróia, um programa malicioso, que é instalado no computador e realiza uma busca

dos dados de forma indevida com o fim específico de subtrair o patrimônio de alguém. Crime de furto e estelionato são outros exemplos que são cometidos por meio da internet que também já eram previstos legislação (DAOUN).

7 O QUE MUDA COM A IMPLEMENTAÇÃO DAS LEIS 12.735 E 12.737, AMBAS DE 2012

A publicação das leis supracitadas não foi de grande relevância para o mundo jurídico. As práticas criminosas no período atual são semelhantes as já tipificadas na legislação. O que mudou foi apenas o *modus operandi*, sendo agora com o auxílio de um computador, *smartphone, tablet*, dentre outros.

A chamada Lei Azeredo, originada do polêmico projeto 84/1999, se apresentou bastante temerosa, pois trazia em seu bojo uma série de vedações capazes de deixar o internauta em um verdadeiro estado de censura, pondo em risco a liberdade deste. Em virtude disto, o projeto sofreu um grande "esvaziamento", restando apenas alguns artigos que, em termos práticos, não trouxeram muitas modificações para o mundo jurídico.

Ainda acerca da lei Azeredo, um fato que deve ser levado em consideração, é que, independente da edição do diploma legal mencionado, existe a reserva do magistrado que já poderia, de oficio, determinar a retirada dos atos dos ilícitos do ar.

Quanto à modernização das delegacias em relação a estas demandas, não é garantia que se implemente tal medida, já que estão atreladas a uma "vontade" da administração pública na esfera do executivo em realizá-la tornando-se mais uma lei "solta no espaço jurídico" sem uma funcionalidade direta.

A lei 12.737/12, batizada de Lei Carolina Dieckmann, alterou o Código Penal, na parte especial, trazendo consigo emprego de termos inadequados ao tipo penal. As penas previstas para esses delitos são exageradamente brandas, ajustadas aos procedimentos realizados nos Juizados Especiais Cíveis. Contra o agente, se provada a violação de sistemas de segurança de computadores por ele, será aberto um TCO - Termo Circunstanciado de Ocorrência – já que se trata de uma infração de menor potencial ofensivo. A guarda dos logs de acesso não é, contemplada, o que tornará difícil a produção de provas para que possa haver o devido enquadramento na figura típica penal. De outra sorte, estamos diante de uma desnecessidade dispondo que, por parte dos nossos legisladores, há uma verdadeira procura pela criação de novos tipos penais, que já são considerados crimes em nosso ordenamento

pátrio. Segundo Caneppele (2015, apud Colli, 2010, pg 184) há dispensabilidade de se criar novos tipos penais aos já existentes quando menciona que “os *cibercrimes* são velhos crimes em novas mídias, ou seja, não há que se falar em crimes que ainda não existem, mas sim em necessária atividade de hermenêutica jurídica baseada na subsunção dos fatos à norma penal incriminadora”.

É importante ressaltar que o Crime Cibernético está investido do princípio da Consunção ou Absorção, ou seja, efetiva-se nos casos em que há uma série de condutas, mas com apenas um nexo dependência. Ocorre que este delito fim absorve o crime meio respondendo o agente a uma pena menor conforme o entendimento da súmula 17 do Supremo Tribunal de Justiça já citada em parágrafos anteriores, *in verbis:* "QUANDO O FALSO SE EXAURE NO ESTELIONATO, SEM MAIS POTENCIALIDADE LESIVA, E POR ESTE ABSORVIDO."

Conforme explanado em parágrafos anteriores, em que a pena para esses crimes são mais brandas, e trazendo à tona a súmula 17, o agente levará a uma depreciação do crime mais grave pelo de menor potencial ofensivo. Isto posto, tomamos ainda como sustentáculo, a decisão do Tribunal Regional Federal da 4ª Região:

> DIREITO PENAL. FURTO QUALIFICADO. SUBTRAÇÃO DE VALORES DE CONTA CORRENTE. FRAUDE PELA INTERNET. LITISPENDÊNCIA NÃO VERIFICADA. DESCLASSIFICAÇÃO PARA INVASÃO DE DISPOSITIVO INFORMÁTICO ALHEIO. ART. 154-A DO CP. NÃO OCORRÊNCIA. AUTORIA COMPROVADA. DOSIMETRIA. SENTENÇA MANTIDA. 1. O objeto da ação penal em trâmite na 2ª Vara da Seção Judiciária do Rio Grande do é distinto do analisado no presente feito. Logo, afasta-se a hipótese de litispendência invocada pela defesa, porque as três operações bancárias objeto deste inquérito não faziam parte da ação penal nº 0007969-66.2007.4.05.8400. 2. Não há falar em desclassificação para o art. 154-A do Código Penal, pois os réus, mediante sua conduta, não apenas "invadiram dispositivo eletrônico alheio para obter vantagem ilícita", tendo efetivamente subtraído a quantia de R$ 3.046,97 (três mil e quarenta e seis reais e noventa e sete centavos) pertencentes à empresa vítima. Incide, por óbvio, o art. 155, §4º, do CP. 3. De acordo com as provas dos autos, o valor foi subtraído, através de fraude eletrônica perpetrada por um dos réus, de conta corrente, agência Ahú/Curitiba/PR da Caixa Econômica Federal, cuja titular é a empresa, vítima do furto. O montante, então, foi direcionado para a conta do outro réu. 4. O réu Paulo Henrique confessou, no interrogatório da investigação. Por sua vez, o acusado James Dean confirmou, em sedes policial e judicial, a prática criminosa, inclusive no que se refere ao codenunciado. 5. Os réus não obtiveram êxito em

> afastar as provas que recaem sobre si, devendo ser mantida a condenação pela prática do crime previsto no art. 155, §4º, II e IV, do Código Penal. 6. Não há o que se reformar na reprimenda aplicada, porquanto corretamente fixada na sentença, inclusive no tocante à substituição das privativas de liberdade por restritivas de direitos.

8 CONCLUSÃO

Restou provado que, o Código Penal existente, é perfeitamente oportuno e cabível, no que diz respeito à tutela dos bens jurídicos que forem transgredidos na rede mundial de computadores. Em síntese, existia sim, uma real necessidade da edição de leis que regulamentassem acerca dos crimes cibernéticos cometidos no meio virtual fazendo-se do uso das tecnologias. Todavia, o que se esperava eram leis com termos mais técnicos e apropriados com o intuito de contemplar as condutas pertinentes a essa pratica criminosa.

A internet é o sinônimo do avanço em comunicações nos dias atuais e vem se expandindo em todas as partes do globo, com uma grande facilidade de acesso, já que os meios são os mais diversificados, interferindo, inclusive, no comportamento e modo de agir de uma sociedade. Nesse ínterim, nasce um novo espaço e consigo novas práticas delituosas ao passo que sem a proteção a esses novos bens jurídicos acompanhe essa nova realidade. Assim, constituem-se novos posicionamentos dos doutrinadores no que diz respeito a essas novas categorias de crime, os puros e os impuros, se distinguindo um do outro pela indispensabilidade do meio tecnológico.

É importante salientar que, para a interpretação, em casos que envolvam a referida prática, se faz necessário o uso do instituto da interpretação extensiva que, ao contrário da analogia, busca a verdadeira finalidade da norma de forma que esta alcance os casos oriundos de crimes cibernéticos. Por essa premissa, o termo “coisa”, inserido nos tipos penais dos artigos 155, 163 e 171, que são os crimes de furto, dano e estelionato, pode ser aplicado para proteger os “dados” informáticos referenciados no artigo 154-A, da lei em comento.

Por fim, as leis em análise demonstram de certa forma, a intenção do legislador em editar leis que venham a punir o agente que pratica esses crimes. Porém nestas deve ser observado as adequações, termos técnicos e específicos, constitucionalidades, inclusive penas mais pertinentes ao dano gerado à vítima. Conclui-se que os dispositivos legais sancionados pelo presidente não são necessários tendo em vista que pelo Código Penal em vigo atualmente, se admite a interpretação extensiva, inclusive aceita pelo Supremo Tribunal Federal.

REFERÊNCIAS

BRASIL. Presidência da República, Subchefia para Assuntos Jurídicos. Lei nº 12.735 de 30 de novembro de 2012. Dispõe sobre tipificação de condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e da outras providencias. Brasília, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm. Acesso em 30 jul. 2016.

BRASIL. Presidência da República, Subchefia para Assuntos Jurídicos. Lei nº 12.737 de 30 de novembro de 2012. Dispõe sobre tipificação criminal de delitos informáticos; altera o Decreto-lei nº 2848, de 7 de dezembro de 1940 - Código Penal; e da outras providencias. Brasília, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 30 jul. 2016.

BRASIL.Supremo Tribunal de Justiça. Súmula n.º 17. QUANDO O FALSO SE EXAURE NO ESTELIONATO, SEM MAIS POTENCIALIDADE LESIVA, E POR ESTE ABSORVIDO. Disponível em: http://www.stj.jus.br/SCON/sumulas/doc.jsp?livre=@num=%2717%27. Acesso em: nov. 2016.

CABETTE, Eduardo Luiz Santos. Primeiras impressões sobre a Lei nº 12.735 e o crime de invasão de dispositivo informático, 2013. Disponível em: https://jus.com.br/artigos/23522/primeiras-impressoes-sobre-a-lei-n-12-737-12-e-o-crime-de-invasao-de-dispositivo-informático. Acesso em 30 jul. 2016.

CANEPPELE.Guilherme Anderson. A (IN) EFICÁCIA DO CRIME DE INVASÃO DE DISPOSITIVO INFORMÁTICO (ART. 154-A DO CÓDIGO PENAL) Lajeado, 2015, p. 56 – 60.

CARNEIRO, Adeneele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. In: **Âmbito Jurídico**, Rio Grande, XV, n. 99, abr 2012. Disponível em: <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=11529>. Acesso em: nov 2016.

CAVALCANTE, Waldek Fachinelli. Crimes Cibernéticos: Noções básicas de investigação e ameaças na internet, 2013. Disponível em: https://jus.com.br/artigos/25743/crimes-ciberneticos/2. Acesso em 30 jul. 2016.

CERT.br. Cartilha de segurança para internet**.** Disponível em:<http://cartilha.cert.br/>. Acesso em: 10.7.2016.

CRESPO, Marcelo. As Leis nº 12.735/2012 e 12.737/2012 e os crimes digitais: acertos e equívocos legislativos. Abr 2015. Disponível em: < http://canalcienciascriminais.com.br/as-leis-no-12-7352012-e-12-7372012-e-os-crimes-digitais-acertos-e-equivocos-legislativos/>. Acesso em: Nov 2016.

DA SILVA, Patrícia Santos. Direito e Crime Cibernético: Análise da Competência em razão do lugar no julgamento de ações penais. Brasília, DF. Editora Vestinik. Disponível em: <https://pensarpoliticamente.files.wordpress.com/2014/02/direito-crime-cibernetico.pdf>. Acesso em: out 2016.

DE ALEXANDRE, Alessandro Rafael Bertollo. Conceito de Crime. Fev 2003. Disponível em: <https://jus.com.br/artigos/3705/o-conceito-de-crime>. Acesso em out 2016.
DUMAS, Véronique. A origem da internet. Revista História viva, São Paulo. Disponível em: <http://www2.uol.com.br/historiaviva/reportagens/o_nascimento_da_internet.html> Acesso em 27 set. 2016.

Em Miniweb Cursos, Conhecendo EAD – Módulo 2, Histórico Internet. Disponível em: <http://www.miniwebcursos.com.br/cursos_antigos/conhecendo_ead/botoes/modulos/modulo_2/artigos/historico_internet.html>. Acesso em: 27. Set. 2016.

FILHO, Odilardo Muniz Lima, DIREITO DIGITAL Crimes Cibernéticos, Teoria e Prática, Maranhão, 2015 (Apostila).
GRECO, Rogério. Curso de Direito Penal: Parte Geral. 14ª Niterói, RJ: Impetus, p. 139 – 145.

Internet já tem quase 3 bilhões de usuários no mundo, diz ONU. Folha de S.Paulo, [SÃO PAULO], 25 novembro. 2014. Disponível em: <http://www1.folha.uol.com.br/tec/2014/11/1553088-internet-ja-tem-quase-3-bilhoes-de-usuarios-no-mundo-diz-onu.shtml>. Acesso em: 27 set. 2016.

LIMA CARVALHO, Paulo Roberto de. Crimes cibernéticos: uma nova roupagem para a criminalidade. Ago 2014. Disponível em:<https://jus.com.br/artigos/31282/crimes-ciberneticos-uma-nova-roupagem-para-a-criminalidade>. Acesso em out 2016.

LIMA, Simão Prado. Crimes virtuais: uma análise da eficácia da legislação brasileira e o desafio do direito penal na atualidade. In: **Âmbito Jurídico**, Rio Grande, XVII, n. 128, set 2014. Disponível em: <http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=15260&revista_caderno=3>. Acesso em: out 2016.

MACIEL, Camila. Tecnologia. Cresce número de denúncias de crimes na internet em 2014. Portal EBC, Brasília, fev 2015. . Disponível em: http://www.ebc.com.br/noticias/2015/02/cresce-numero-de-denuncias-de-crimes-na-internet-em-2014. Acesso em Nov 2016.

Ministério Público Federal. **Crimes cibernéticos:** Manual prático de investigação. São Paulo: Procuradoria da República no Estado de SP, 2006.
MUTA, Luiz Carlos Hiroki. **Direito Constitucional**. Tomo I. Rio de Janeiro: Elsevier, 2007. Disponível em: <http://books.google.com.br/books?id=gQxfw_V_RJQC&pg=PA128&dq=Princ%C3%ADpio+do+Estado+de+Inoc%C3%AAncia&hl=en&sa=X&ei=6MNNUo_fDZDQ9gSl0IEw&ved=0CE4Q6AEwBQ#v=onepage&q&f=true> Acesso em 20 nov 2016, p. 128.

Portal ABRANET – Associação Brasileira de Internet. Notícias, Abranet Responde: o que é Internet, o que é serviço de telecom e quando é preciso ter autorização. Disponível em:

http://www.abranet.org.br/Noticias/Abranet-Responde%3A-o-que-e-Internet,-o-que-e-servico-de-telecom-e-quando-e-preciso-ter-autorizacao-438.html#.WCutjeYrLIU>. Acesso em: Nov 2016.

Portal CNF – Confederação Nacional das Instituições Financeiras. Notícias, Aprovado projeto de crimes eletrônicos. Disponível em: < http://www.cnf.org.br/noticia/-/blogs/aprovado-projeto-de-crimes-eletronicos>. Acesso em: nov 2016.

Portal Idgnow, 3,2 bilhões de pessoas no mundo todo usam Internet, diz Facebook. Disponível em: <http://idgnow.com.br/internet/2016/02/24/3-2-bilhoes-de-pessoas-no-mundo-todo-usam-internet-diz-facebook/>. Acesso em: 27 set. 2016**.**

PRADO, Luis Regis. **Curso de Direito Penal Brasileiro**: Parte Geral. 10ª ed. São Paulo: Editora Revista dos Tribunais, 2010, p.116-118.

SIENA, David Pimentel Barbosa de. Lei Carolina Dieckmann e a definição de "crimes virtuais", 2013. Disponível em: https://jus.com.br/artigos/24406/lei-carolina-dieckmann-e-a-definição-de-crimes-virtuais. Acesso em 30 jul. 2016.

SILVA, Camila Requião Fentanes da. Análise das Leis nº 12.735/2012 e 12.737/2012 e a (des)necessidade de uma legislação específica sobre crimes cibernéticos, 2014. Disponível em: https://jus.com.br/artigos/32265/analise-das-leis-n-12-735-2012-e-desnecessidade-de-uma-legislação-específica-sobre-crimes-ciberneticos. Acesso em 30 jul. 2016.

SILVEIRA, Artur Barbosa da. Os crimes cibernéticos e a Lei 12.737/2012, 2015. Disponível em: http://www.conteudojuridico.com.br/artigo,os-crimes-ciberneticos-e-a-lei-no-127372012,52253.html. Acesso em 30 ago. 2016.

TELES, Tayson Ribeiro. TIC´s, Crimes Cibernéticos e a Lei Federal nº 12.737/2012: ações e prevenções, 2015. Disponível em: www.conteudojuridico.com.br/artigo,tics-crimes-ciberneticos-e-a-lei-federal-no-127372012-açoes-e-prevençoes,53281.html. Acesso em 30 jul. 2016.

VELLOSO, Jean Pablo Barbosa. Crimes Informáticos e Criminalidade Contemporânea. Out. 2015. Disponível em: <http://www.jurisway.org.br/v2/dhall.asp?id_dh=15756>. Acesso em: out 2016.

VIANNA, Túlio Lima. **Dos crimes pela internet**. Disponível em: <http://www.academia.edu/1911162/Dos_crimes_pela_internet> Acesso em: Nov 2013, p.5.