UNIVERSIDADE FEDERAL DE CAMPINA GRANDE – UFCG
CENTRO DE CIÊNCIAS JURÍDICAS E SOCIAIS – CCJS
UNIDADE ACADÊMICA DE DIREITO

VINICIUS CEZAR DE MOURA PEREIRA

OS CIBERCRIMES E A LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012: UMA ANÁLISE ACERCA DE SUA EFICÁCIA NO COMBATE AO CIBERCRIME E SEUS ASPECTOS JURÍDICOS.

.

SOUSA
2014

VINICIUS CEZAR DE MOURA PEREIRA

OS CIBERCRIMES E A LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012: UMA ANÁLISE ACERCA DE SUA EFICÁCIA NO COMBATE AO CIBERCRIME E SEUS ASPECTOS JURÍDICOS.

Trabalho monográfico apresentado ao Curso de Direito do Centro de Ciências Jurídicas e Sociais da Universidade Federal de Campina Grande, como exigência parcial da obtenção do título de Bacharel em Ciências Jurídicas e Sociais.

Orientador: Prof. Cícero Marcelo Bezerra dos Santos.

SOUSA

2014

VINICIUS CEZAR DE MOURA PEREIRA

OS CIBERCRIMES E A LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012: UMA ANÁLISE ACERCA DE SUA EFICÁCIA NO COMBATE AO CIBERCRIME E SEUS ASPECTOS JURÍDICOS.

Trabalho monográfico apresentado ao Curso de Direito do Centro de Ciências Jurídicas e Sociais da Universidade Federal de Campina Grande, como exigência parcial da obtenção do título de Bacharel em Ciências Jurídicas e Sociais.

Orientador: Prof. Cícero Marcelo Bezerra dos Santos

Banca Examinadora: Data de Aprovação:

_____

Título – Professor – Instituição

_____

Título – Professor – Instituição

_____

Título – Professor – Instituição

Aos meus pais FRANCISCO e
MARIA pelo eterno incentivo.

AGRADECIMENTOS

Aos meus pais, Maria e Francisco, por todo amor, carinho e dedicação.

A minha namorada Áquila, que me ajuda o tempo todo e alegra minha vida, sempre me levando a buscar os caminhos mais certos.

Ao professor Cícero Marcelo, grande orientador pelo apoio na consecução deste trabalho também aos professores Paulo Abrantes, Iranilton Trajano e Iarley.

Aos meus parentes, Priscila, Naila, Sara, Clara e Justino para quem tenho grande consideração além Carlos e Wesley por todo o apoio.

Aos meus familiares como um tudo pois, sempre me deram o exemplo de que só através do estudo que se pode prosseguir na vida.

Aos meus amigos da faculdade, Lívio, Istélio, Juliana, Sara, Suellen, Graciene e Barbara com os quais passei muitos momentos, ao longo desses cinco anos.

Aos meus companheiros de viagem, que sempre ajudaram a manter o ânimo em todas as tardes que fizemos o percurso Sousa-Cajazeiras.

“O problema não é se as máquinas pensam,
mas se os homens fazem”
B.F. Skinner.

RESUMO

A evolução tecnológica da informática e da forma de compartilhamento de informações romperam paradigmas com o passar do tempo e estabeleceram novas tecnologias de organização desta estrutura. Particularmente, após a criação da "World Wide Web" por Tim Berners Lee em 1990 a produção e compartilhamento de informações multiplicaram-se exponencialmente na rede necessitando assim de alguma legislação específica para regulamentar e proteger os conteúdos compartilhados. A Constituição Federal de 1988, ao tratar dos direitos e garantias fundamentais, em seu artigo 5º, assegura, dentre os direitos e deveres individuais e coletivos, o direito à privacidade e o direito ao acesso a informação, só que de ambos surgiu uma celeuma que trata dos cibercrimes, ou seja, dos crimes cometidos na esfera dos meios informáticos. Em face do aumento das condutas delituosas ocorridas no meio cibernético o legislador se viu na posição de elaborar leis que regulem e reprimam tais condutas, e deste ensejo surgiu a lei nº 12.737/2012 que versa sobre os delitos informáticos. Nesta esteira, a presente pesquisa, tem por escopo analisar a mencionada, de forma a verificar se esta tem se mostrado eficaz no combate e repressão aos cibercrimes, e se está se mostrou aplicável no contexto atual dos delitos ocorridos nos meios cibernéticos. O Método de abordagem utilizado na pesquisa científica será o dedutivo; a pesquisa terá como métodos de procedimento o monográfico, crítico e analítico e a técnica de pesquisa será a documentação indireta abrangendo a pesquisa bibliográfica.

Palavras-chave: Cibercrimes. Dispositivos Informáticos. Internet. Informática Jurídica.

ABSTRACT

The technological evolution of computing and way of information sharing broke paradigms over time and established new technologies of organization of this structure. Particularly, after the creation of the “World Wide Web " by Tim Berners Lee in 1990 to publish and share information have multiplied exponentially in the network thus requiring any specific legislation to regulate and protect the shared content . The Federal Constitution of 1988, in order to take care the rights and guarantees in its Article 5 ensures, among the rights and individual and collective obligations , the right to privacy and the right to access the information , only that both arose a stir dealing of cybercrime , in other words , crimes committed in the sphere of computer equipment. In the face of increased cybercriminal conduct occurred in the middle of the legislature was drafting laws regulating position and suppress such conduct , and this opportunity to Law No. 12.737/2012 which deals with computer crimes emerged . On this track , the present research is to analyze the scope mentioned in order to verify that this has been proven effective in fighting and repression of cybercrime , and is proved to be applicable in the current context of the offenses occurred in cyber means. The method of approach used in scientific research is deductive, as will research methods of procedure the monographic, critical, analytical, and technical research will be indirectly documentation covering the literature.

Keywords: Cybercrime. Computer devices. Internet. Cyber Law.

LISTA DE ABREVIATURAS E SIGLAS

CCJS – Centro de Ciências Jurídicas e Sociais
CF – Constituição Federal
PL – Projeto de Lei
UFCG – Universidade Federal de Campina Grande
ART – Artigo
ENIAC – Eletronic Numeric Integrator and Calculator.
CPU – Central Processing Unit (Unidade Central de Processamento)
IBM – International Business Machines (Máquinas Internacionais de Negócio)
BIOS – Basic Input/Output System (Sistema Básico de Entrada/Saída).
ARPA – Advanced Research Project Agency (Agência de Projetos de Pesquisa Avançados)
TCP – Transmission Control Protocol (Protocolo de Controle de Transmissão)
HTTP – Hyper Text Transfer Protocol (Protocolo de Transferência de Hyper Texto)
HTML – Hyper Text Markup Language (Linguagem de Marcação de Hyper Texto)
RNP – Rede Nacional de Ensino e Pesquisa
IP – Internet Protocol (Protocolo de Internet)
Gbps – Gigabytes por segundo
IBGE – Instituto Brasileiro de Geografia e Estatística RAM
PC – Personal Computer (Computador Pessoal)
SPAM – Sending and Posting Advertisement in Mass
DoS – Denial of Service (Negação de Serviço)

SUMÁRIO

1 INTRODUÇÃO.

Os direitos individuais podem ser considerados a maior conquista da sociedade, posto que estes transformaram de sobremaneira o convívio social, entre esses direitos individuais, está o direito a um espaço privativo do cidadão, ou seja, o lugar o qual ele necessidade desfrutar da a privacidade. A necessidade de se proteger a vida privada surgiu da conflitante relação entre o indivíduo e a sociedade, tal conflito existe na sociedade atualmente em larga escala, por conta do uso ampliado da internet, onde cada vez a privacidade vai se perdendo e que os cibercrimes justamente que violam a privacidade de terceiros buscando a obtenção de seus dados se tornaram uma prática crescente de forma que recentemente entrou em vigor a lei nº 12.737/2012.

A escolha do tema desta pesquisa dá-se diante de se fazer necessária a análise da supracitada lei, onde aqui se caberá analisar se ela cumprirá o seu papel como reguladora dos cibercrimes, posto que esta não só acresceu o Código Penal nos art. 154-A e 154-B e alterou a redação dos art. 266 e 298, buscando abranger essas condutas delituosas.

Posto isto se têm como principais objetivos do presente trabalho, apontar possíveis falhar nos dispositivos legais e apontar se esta lei será eficaz na repressão a conduta típica dos cibercrimes. Analise da Lei nº 12.737/2012, abordando sua aplicação e se esta se tornou eficaz para regular os crimes ocorridos no meio eletrônico. Verificar a aplicabilidade e eficácia da lei nº 12.737/2012, explicar se o conteúdo da norma corresponde à realidade social, identificar possíveis falhas no texto legal que venham a limitar a sua aplicação e que podem vir a torná-la ineficaz para regular e punir os crimes cibernéticos, que são aqueles crimes cuja execução ocorre no meio digital.

O Método de abordagem utilizado nessa pesquisa científica será o dedutivo, baseando-se na aplicação de princípios, teorias e leis genéricas em fenômenos mais específicos.

A pesquisa terá como métodos de procedimento o monográfico, crítico e analítico, investigando o tema em diversos aspectos de forma completa e sistemática, analisando os dispositivos que compõe do texto da lei nº 12.737/2012 apontando suas possíveis falhas e se está sendo eficaz na repressão aos cibercrimes.

A técnica de pesquisa será a documentação indireta abrangendo a pesquisa bibliográfica, por meio da utilização de leis, tratados internacionais, livros e artigos científicos.

Num primeiro momento se fez uma abordagem histórica, em que se apresentou desde os primórdios das primeiras máquinas de computar, e seu desenvolvimento através do tempo, expondo quais foram os principais marcos em sua história e que nomes contribuíram para sua evolução.

Apontou-se também o momento em que surgiu o primeiro computador que se adequou a concepção moderna de computador e quais foram suas aplicações iniciais. Procurou-se dessa forma estabelecer um conceito do que seria o dispositivo informático, que no caso em análise seriam os computadores e demais dispositivos que possuímos com a capacidade de processar informação e como este se caracteriza no que foi apontada como sendo a quinta geração de computadores.

Ademais, explanou-se sobre o início da internet, tratando desde sua origem inicialmente militar, e como esta se tornou a forma de comunicação mais revolucionária da humanidade. Também se apontou como foi a entrada da internet no Brasil e que atualmente ela se tornou utilizada por mais de 100 milhões de brasileiros, conforme dados divulgados pelo IBGE em 2013.

E isto se fez no intuito de se delinear o plano de fundo para o tema aqui tratado que é o dos cibercrimes posto que estes ocorrem num plano paralelo mas, intimamente ligado a nossa sociedade.

Em seguida no capítulo seguinte se passou a explanar outro componente deste trabalho que é o dos cibercrimes, se apresentando um conceito e uma análise desta figura, se avaliando inclusive se este assume a figura da tentativa ou a modalidade culposa, além de descrever os principais tipos de criminosos digitais abordando figuras como a do *hacker* e do *cracker,* as principais ameaças que se encontram no mundo cibernético, falando-se logo após sobre os *hackers* mais famosos, e isso se fez no sentido de que estes são os maiores influenciadores da conduta ilícita na internet.

Tratou-se logo em seguida sobre *Hacktivismo,* dado que este se tornou uma tendência cada vez maior na atualidade dada a grande repercussão da mídia online e que esses ataques ganharam um papel de protesto político.

Dissertou-se também sobre Engenharia Social, tanto pelo fato desta ter se tornado a prática mais utilizada na realização de cibercrimes, como pela forma que se configura na atualidade, se unindo as figuras do *spam* e do *phishing.*

Outro ponto que se destacou foi o das formas de combate ao cibercrime no Brasil, de forma que se apontou quais órgão são responsáveis pelo combate ao cibercrime, e como está a atual situação brasileira, posto que se denotou que existem uma série de dificuldades no tocante a existência de uma investigação unificada, através da cooperação mútua entre os estados, e da necessidade da criação de um banco de dados nacional que sirva para auxiliar em futuras investigações.

Logos após, se tratou acerca do diploma legal cuja criação ensejou este trabalho monográfico, que é o da Lei nº 12.737/12, se fez de forma inicial um breve histórico da situação que foi a mola propulsora para a aprovação em tempo recorde do diploma, e de como este surgiu na verdade tratando de crimes de natureza diversa do fato pelo qual ganhou notoriedade.

Após isto se procedeu com um estudo do tipo penal, invasão de dispositivo informático alheio, onde se buscou apresentar os tipos objetivo e subjetivos que se encontram presentes nesta nova conduta que foi tipificada, analisou-se também os sujeitos ativo e passivo do tipo, bem como se buscou demonstrar quando ocorre a consumação e se é possível existir a tentativa e a modalidade culposa.

Se abordou também que num único tipo se inseriram também figuras que foram equiparadas ao ilícito, além de se fazer uma análise acerca das possíveis causas de aumento de pena além de sua forma qualificada.

E por fim se expôs as críticas que surgiram em razão desse texto legal, principalmente por se tratar de uma figura nova em nosso ordenamento jurídico e que ainda possui certas dificuldade na interpretação de seu texto e na sua aplicabilidade ao caso concreto.

2 O SURGIMENTO DA ERA INFORMÁTICA.

Sem sombra de dúvidas o computador e seus derivados se demonstraram como algumas das invenções que mais modificaram o cotidiano. E isso se pode evidenciar de forma que, ao se olhar desde os primórdios, em que desenvolveram os primeiros aparatos como o intuito de ajudar no ato de calcular, até os dias de hoje em que possuímos em nossos bolsos computadores com poder de processamento de informação que vai além, do que podemos imaginar.

E juntamente com tais máquinas surgiu a internet, que numa velocidade ainda maior se entrelaçou no cotidiano de forma se tornar indispensável, não só pela forma como a internet mudou as comunicações as tornando mais ágeis e práticas como também na forma de compartilhar dados.

De toda forma, para se entender com profundidade como se modelou essa atual realidade moldada por máquinas, estas que já desempenham funções de vital importância na vida em sociedade deve-se voltar dos seus primórdios analisando como estas se transformaram no decorrer do tempo.

2.1 O SURGIMENTO DAS PRIMEIRAS MÁQUINAS DE COMPUTAR ATÉ O COMPUTADOR MODERNO.

Segundo Fonseca Filho (2007, p.85-92) podemos delinear a história da computação, partindo do fato de que os primeiros dispositivos que surgiram para ajudar o homem a calcular têm sua origem perdida nos tempos. É o caso, por exemplo, do ábaco e do quadrante. O primeiro, capaz de resolver problemas de adição, subtração, multiplicação e divisão de até 12 inteiros, e que provavelmente já existia na Babilônia por volta do ano 3.000 A.C. Foi muito utilizado pelas civilizações egípcia, grega, chinesa e romana, tendo sido encontrado no Japão, ao término da segunda guerra mundial.

O quadrante era um instrumento para cálculo astronômico, tendo existido por centenas de anos antes de se tornar objeto de vários aperfeiçoamentos. Os antigos babilônios e gregos como, por exemplo, Ptolomeu, usaram vários tipos de dispositivos desse tipo para medir os ângulos entre as estrelas, tendo sido desenvolvidos principalmente a partir do século

XVI na Europa. Outro exemplo é o compasso de setor, para cálculos trigonométricos, utilizado para se determinar a altura para o posicionamento da boca de um canhão, e que foi desenvolvido a partir do século XV. A mais antiga ferramenta conhecida para uso em computação como sendo o ábaco, e foi inventado na Babilônia por volta de 3.000 A.C.

Ainda segundo o mesmo autor podemos apontar John Napier, pela descoberta dos logaritmos, mas também gastou grande parte de sua vida inventando instrumentos para ajudar no cálculo aritmético, principalmente para o uso de sua primeira tabela de logaritmo.

A partir dos logaritmos de Napier surgiu uma outra grande invenção, desenvolvida pelo brilhante matemático Willian Oughtred e tornada pública em 1630: a régua de cálculo.

Ganhou sua forma atual por volta do ano de 1650 (de uma régua que se move entre dois outros blocos fixos), tendo sido esquecida por duzentos anos, para se tornar no século XX o grande símbolo de avanço tecnológico, com uso extremamente difundido, até ser definitivamente substituída pelas calculadoras eletrônicas.

Com o desenvolvimento dos primeiros dispositivos mecânicos para cálculo automático, começa efetivamente a vertente tecnológica que levará à construção dos primeiros computadores.

A primeira máquina de verdade foi construída por Wilhelm Schickard (1592-1635), sendo capaz de somar, subtrair, multiplicar e dividir. Essa máquina foi perdida durante a guerra dos trinta anos, sendo que recentemente foi encontrada alguma documentação sobre ela. Durante muitos anos nada se soube sobre essa máquina, por isso, atribuía-se a Blaise Pascal (1623-1662) a construção da primeira máquina calculadora, que fazia apenas somas e subtrações, que desenvolveu a máquina para auxiliar o seu trabalho de contabilidade, a calculadora usava engrenagens que a faziam funcionar de maneira similar a um odômetro[1]. Mais adiante durante a Revolução Industrial em 1801, na França, Joseph Marie Jacquard, mecânico francês inventou um tear mecânico controlado por grandes cartões perfurados.

[1] **Odómetro/odômetro ou hodómetro/hodômetro**: é um equipamento destinado a medir a distância percorrida por um veículo. Normalmente ele é indicado no visor com a palavra "ODO" para distância total e "DST" para distâncias parciais. O velocímetro trabalha em conjunto com o odômetro, pois o cálculo é feito entre a distância percorrida e o tempo em questão, gerando a velocidade atual. Hoje em dia, a função do hodômetro pode ser realizada também através do GPS.

O computador moderno começou a ganhar forma Charles Babbage que, através de seu trabalho no engenho analítico. O equipamento, apesar de nunca ter sido construído com sucesso, possuía todas as funcionalidades do computador moderno. Foi descrito originalmente em 1837, mais de um século antes que qualquer equipamento do gênero tivesse sido construído com sucesso. O grande diferencial do sistema de Babbage era o fato que seu dispositivo foi projetado para ser programável, item imprescindível para qualquer computador moderno.

Durante sua colaboração, a matemática Ada Lovelace (1815-1852) publicou os primeiros programas de computador em uma série de notas para o engenho analítico. Por isso, é popularmente considerada como a primeira programadora.

O Autor ainda destaca que em 1946, o engenheiro John Presper Eckert e o físico John Mauchly projetaram o ENIAC: *Eletronic Numeric Integrator And Calculator*. Com 18 000 válvulas, o ENIAC conseguia fazer 500 multiplicações por segundo que os custos para a manutenção e conservação do ENIAC eram proibitivos, pois dezenas a centenas de válvulas queimavam a cada hora e o calor gerado por elas necessitava ser controlado por um complexo sistema de refrigeração, além dos gastos elevadíssimos de energia elétrica.

No ENIAC, o programa era feito rearranjando a fiação em um painel. Nesse ponto John von Neumann propôs a ideia que transformou os calculadores eletrônicos em "cérebros eletrônicos": tal ideia consiste em modelar a arquitetura do computador segundo o sistema nervoso central, de forma que este pudesse fazer diversas operações de forma integrada. Para isso, eles teriam que obter três características: Codificar as instruções de uma forma possível de ser armazenada na memória do computador. Von Neumann sugeriu que fossem usados uns e zeros. Armazenar as instruções na memória, bem como toda e qualquer informação necessária a execução da tarefa e quando processar o programa, buscar as instruções diretamente na memória, ao invés de lerem um novo cartão perfurado a cada passo.

Este é o conceito de programa armazenado, cujas principais vantagens são: rapidez, versatilidade e auto modificação. Assim, o computador programável que conhecemos hoje, onde o programa e os dados estão armazenados na memória ficou conhecido como Arquitetura de von Neumann.

Antes da década de 1920, o computador era um termo associado a pessoas que realizavam cálculos, geralmente liderados por físicos em sua maioria homens.

Milhares de computadores, eram empregados em projetos no comércio, governo e sítios de pesquisa. Após a década de 1920, a expressão máquina computacional começou a ser usada para se referir a qualquer máquina que realize o trabalho de um profissional computador, especialmente aquelas de acordo com os métodos da Tese de Church-Turing.

O termo máquina computacional acabou perdendo espaço para o termo reduzido computador no final da década de 1940, com as máquinas digitais cada vez mais difundidas. Alan Turing, conhecido como pai da Ciência da Computação, inventou a Máquina de Turing, que posteriormente evoluiu para o computador moderno.

Até o final dos anos 1970, segundo Fonseca Filho (2007) reinavam absolutos os mainframes, computadores enormes, trancados em salas refrigeradas e operados apenas por alguns poucos privilegiados. Apenas grandes empresas e bancos podiam investir alguns milhões de dólares para tornar mais eficientes alguns processos internos e o fluxo de informações. A maioria dos escritórios funcionava mais ou menos da mesma maneira que no começo do século. Arquivos de metal, máquinas de escrever, papel carbono e memorandos faziam parte do dia-a-dia.

Em 1971 surgiu o primeiro "computador pessoal" que foi o Kenbak-1**,** tinha 256 bytes de memória e foi anunciado na revista Scientific American por US$ 750; todavia, não possuía CPU e era, como outros sistemas desta época, projetado para uso educativo (ou seja, demonstrar como um "computador de verdade" funcionava). Em 1975, surge o Altair 8800, um computador pessoal baseado na CPU Intel 8080. Vendido originalmente como um kit de montar através da revista norte-americana Popular Electronics, os projetistas pretendiam vender apenas algumas centenas de unidades, tendo ficado surpresos quando venderam 10 vezes mais que o previsto para o primeiro mês. Custava cerca de 400 dólares e se comunicava com o usuário através de luzes que piscavam. Entre os primeiros usuários estavam Bill Gates, e o jovem programador, Paul Allen, que juntos desenvolveram uma versão da linguagem "Basic" para o Altair, e que mais tarde estes vieram a fundar a Microsoft.

Em 1976, outra dupla formada por Steve Jobs e Steve Wozniak, iniciou outra empresa que mudaria o rumo da informática: a Apple. Em 1977, foi lançado o primeiro microcomputador como conhecemos hoje, o Apple II. O equipamento já vinha montado, com teclado integrado ao monitor, de forma que era um dispositivo único e era capaz de gerar gráficos coloridos. Parte da linguagem de programação

do Apple II havia sido feita pela Microsoft, uma variação do BASIC para o Apple II. As vendas chegaram a US$ 2,5 milhões no primeiro ano de comercialização e, com o seu rápido crescimento de vendas, a Apple tornou-se uma empresa.

Em 1980, a IBM adentrou no mercado de produção de computadores voltados para o meio corporativo, e lançou o IBM-PC, que criou uma mudança no conceito que se tinha de computadores corporativos e se demonstrou um grande sucesso.

Em dezembro de 1979, a Apple Computer era a empresa de maior sucesso da microinformática. O carro chefe da empresa, o Apple II+ já estava presente em escolas e residências da elite americana. Entretanto, as máquinas ainda eram difíceis de usar. Para operar um microcomputador, era preciso conhecer a "linguagem" do sistema operacional e a sintaxe correta para aplicá-la. Todas as interações do usuário com a máquina eram feitas através da digitação de comandos. Uma letra errada e a operação não era realizada, exigindo a digitação do comando correto. Assim, antes de aproveitar os benefícios da informática, era indispensável aprender todos os comandos de controle do computador.

Ainda em 1979 Jef Raskin, um especialista em interfaces homem-máquina, imaginou um computador fácil de utilizar e barato para o grande público. Ele então lançou as bases do projeto Macintosh. O projeto inovador do Macintosh atraiu a atenção de Steve Jobs, que saiu do projeto Lisa com sua equipe para se concentrar no projeto Macintosh. Em janeiro de 1981, ele tomou a direção do projeto, forçando Jef Raskin a deixar o mesmo.

Em 24 de janeiro de 1984 surgiu o Macintosh, o primeiro computador de sucesso com uma interface gráfica amigável, usando ícones, janelas e mouse. Sua acolhida foi extremamente entusiástica, grande parte disso devido as campanhas publicitárias em massa da Apple.

O mesmo grupo que criou o IBM-PC também definiu que o componente básico do computador, a BIOS, seria de fabricação exclusiva da IBM. Esse chip tem a finalidade de fornecer aos PCs uma interface de entrada e saída de dados. Como todos os outros componentes do computador eram fabricados por outras empresas, a IBM tinha nesses chips a sua maior fonte de renda e a única coisa que vinculava qualquer PC à IBM.

Algumas empresas, dentre elas a Compaq, aplicaram a técnica de engenharia reversa no BIOS, clonaram-na e construíram computadores similares ao

da IBM. Em novembro de 1982, a Compaq anuncia o Compaq Portable, primeiro PC que não usa a BIOS da IBM e mantém 100% de compatibilidade com o IBM PC.

Esses computadores são conhecidos como "IBM PC compatíveis" e são os PCs que são vendidos nas lojas até hoje, apenas bem mais evoluídos do que os primeiros PCs. Isso levou a IBM a se tornar uma simples empresa que fabricava computadores pessoais e concorria como qualquer outra nesse mercado. A IBM praticamente abandonou o mercado de PCs e se dedicou ao mercado de servidores, na qual é imbatível até hoje.

Através dessa linha histórica se estabeleceram as gerações de computadores que se dividem através de seus componentes de hardware e de sua capacidade de processamento.

Ainda segundo Fonseca Filho (2007) temos que as três primeiras gerações de computadores refletiam a evolução dos componentes básicos do computador (hardware) e um aprimoramento dos programas (software) existentes.

Os computadores de primeira geração (1945–1959) usavam válvulas eletrônicas, quilômetros de fios, eram lentos, enormes e esquentavam muito.

A segunda geração (1959–1964) substituiu as válvulas eletrônicas por transístores e os fios de ligação por circuitos impressos, o que tornou os computadores mais rápidos, menores e de custo mais baixo.

A terceira geração de computadores (1964–1970) foi construída com circuitos integrados, proporcionando maior compactação, redução dos custos e velocidade de processamento da ordem de microssegundos. Tem início a utilização de avançados sistemas operacionais.

A quarta geração, de 1970 até hoje, é caracterizada por um aperfeiçoamento da tecnologia já existente, proporcionando uma otimização da máquina para os problemas do usuário, maior grau de miniaturização, confiabilidade e maior velocidade, já da ordem de nano segundos (bilionésima parte do segundo).

O termo quinta geração foi criado pelos japoneses para descrever os potentes computadores "inteligentes" que queriam construir em meados da década de 1990. Posteriormente, o termo passou a envolver elementos de diversas áreas de pesquisa relacionadas à inteligência computadorizada: inteligência artificial, sistemas especialistas e linguagem natural.

Mas o verdadeiro foco dessa ininterrupta quinta geração é a conectividade, o maciço esforço da indústria para permitir aos usuários conectarem seus computadores a outros computadores.

No início do século XXI, a partir de iniciativas de empresas como o Google, a Nokia e, sobretudo, a Apple, iniciaram uma extensão da quarta geração de computadores que resultou na unificação de linguagens de tecnologias já existentes, e consequente extensão das funcionalidades. A computação pessoal deixou de se limitar aos chamados desktops (outrora chamados de "microcomputadores") e passou a incluir outros dispositivos como telefones celulares e aparelhos de televisão, bem como uma nova categoria de dispositivos chamado tablet - uma espécie de computador delgado e portátil, sem teclado físico nem mouse e com tela sensível ao toque, do tamanho de um livro. Aplicações de uso geral passaram a ser portadas para esses dispositivos e, devido ao desenvolvimento da computação em nuvem, arquivos armazenados em um dispositivo puderam ser sincronizados em outros dispositivos, tornando a computação onipresente. Estes conceitos, que estão em curso atualmente, estão progressivamente tornando mídias físicas externas obsoletas, salvo talvez os cartões de memória.

2.2 O SURGIMENTO DA INTERNET

A internet teve seu início no final dos anos 1960, durante a Guerra Fria, graças à iniciativa do Departamento de Defesa americano, que queria dispor de um conjunto de comunicação militar entre seus diferentes centros.

Para isso, o pesquisador Paul Baran concebeu um conjunto que teria como base um sistema descentralizado. Esse cientista é considerado um dos principais pioneiros da internet. Ele pensou em uma rede na qual os dados se movessem buscando a melhor trajetória possível, podendo “esperar” caso as vias estivessem obstruídas. Essa nova tecnologia, sobre a qual também se debruçaram outros grupos de pesquisadores americanos, foi batizada de *packet switching*, “troca de pacotes”.

Em 1969, a rede ARPAnet já estava operacional. Ela foi o fruto de pesquisas realizadas pela *Advanced Research Project Agency* (ARPA), um órgão ligado ao Departamento de Defesa americano. A ARPA foi criada pelo presidente americano

Eisenhower em 1957, depois do lançamento do primeiro satélite Sputnik pelos soviéticos, para realizar projetos que garantissem aos Estados Unidos a superioridade científica e técnica sobre seus rivais do leste.

A ARPAnet a princípio conectaria as universidades de Stanford, Los Angeles, Santa Barbara e de Utah. Paralelamente, em 1971, o engenheiro americano Ray Tomlinson criou o correio eletrônico. No ano seguinte, Lawrence G. Roberts desenvolveu um aplicativo que permitia a utilização ordenada dos e-mails. As mensagens eletrônicas se tornaram o instrumento mais utilizado da rede. A ARPAnet seguiu sua expansão durante os anos 1970 – a parte de comunicação militar da rede foi isolada e passou a se chamar MILnet.

Outras redes, conectando institutos de pesquisas, foram criadas nos Estados Unidos, Grã-Bretanha e França. Faltava estabelecer uma linguagem comum a todas. Isso foi feito com o protocolo TCP/IP, inventado por Robert Kahnet e Vint Cerf em 1974. A ARPAnet adotou essa padronização em 1976.

Em 1990 com a criação, do protocolo HTTP (Hyper Text Transfer Protocol) e da linguagem HTML (Hyper Text Markup Language) por um pesquisador do Conselho Europeu para a Pesquisa Nuclear em Genebra (Cern), Tim Berners-Lee, que permitem navegar de um site a outro, ou de uma página a outra. A *World Wide Web* e a internet se abriu ao público, empresas particulares e privadas. Uma multidão de sites apareceu.

A partir de 1993 a Internet deixou de ser uma instituição de natureza apenas acadêmica e passou a ser explorada comercialmente, tanto para a construção de *backbones*[2] por empresas privadas (PSI, UUnet, Sprint) como para fornecimento de serviços diversos, abertura essa a nível mundial.

2.3 A INTERNET NO BRASIL

No Brasil, os primeiros embriões de rede surgiram em 1988 e ligavam universidades do Brasil a instituições localizadas nos Estados Unidos. No mesmo ano, o Ibase começou a testar o Alternex, o primeiro serviço brasileiro de Internet não acadêmica e não governamental.

[2] No contexto de redes de computadores, o backbone (backbone traduzindo para português, espinha dorsal, embora no contexto de redes, backbone signifique rede de transporte) designa o esquema de ligações centrais de um sistema mais amplo, tipicamente de elevado desempenho.

Em 1989, o Ministério da Ciência e Tecnologia lança um projeto pioneiro, a Rede Nacional de Ensino e Pesquisa (RNP). Existente ainda hoje, a RNP é uma organização de interesse público cuja principal missão é operar uma rede acadêmica de alcance nacional. Quando foi lançada, a organização tinha o objetivo de capacitar recursos humanos de alta tecnologia e difundir a tecnologia Internet através da implantação do primeiro backbone nacional.

O backbone funciona como uma espinha dorsal, é a infraestrutura que conecta todos os pontos de uma rede. O primeiro backbone brasileiro foi inaugurado em 1991, destinado exclusivamente à comunidade acadêmica. Mais tarde, em 1995, o governo resolveu abrir o *backbone* e, fornecer conectividade a provedores de acesso comerciais. A partir dessa decisão, surgiu uma discussão sobre o papel da RNP como uma rede estritamente acadêmica com acesso livre para acadêmicos e taxada para todos dos outros consumidores. Com o crescimento da Internet comercial, a RNP voltou novamente a atenção para a comunidade científica.

A partir de 1997, iniciou-se uma nova fase na Internet brasileira. O aumento de acessos a rede e a necessidade de uma infraestrutura mais veloz e segura levou a investimentos em novas tecnologias. Entretanto, devido a carência de uma infraestrutura de fibra óptica que cobrisse todo o território nacional, primeiramente, optou-se pela criação de redes locais de alta velocidade, aproveitando a estrutura de algumas regiões metropolitanas. Como parte desses investimentos, em 2000, foi implantado o backbone RNP2 com o objetivo de interligar todo o país em uma rede de alta tecnologia. Atualmente, o RNP2 conecta os 27 estados brasileiros e interliga mais de 300 instituições de ensino superior e de pesquisa no país, como o INMETRO e suas sedes regionais.

Outro avanço alcançado pela RNP ocorreu em 2002. Nesse ano, o então presidente da república transformou a RNP em uma organização social. Com isso ela passa a ter maior autonomia administrativa para executar as tarefas e o poder público ganha meios de controle mais eficazes para avaliar e cobrar os resultados. Como objetivos dessa transformação estão o fornecimento de serviços de infraestrutura de redes IP avançadas, a implantação e a avaliação de novas tecnologias de rede, a disseminação dessas tecnologias e a capacitação de recursos humanos na área de segurança de redes, gerência e roteamento.

A partir de 2005, a comunicação entre os point of presence (PoPs), que traduzidos do inglês significa pontos de presença, eles desempenham o papel de

roteadores que intermediam a comunicação entre os servidores de internet, e com esta nova tecnologia da rede, ampliada com o uso de tecnologia óptica, se elevou a capacidade de operação a 11 Gbps.

A internet revolucionou o funcionamento tradicional das sociedades modernas como o fizeram, a seu tempo, a imprensa, a máquina a vapor, a eletricidade ou a telegrafia sem fio (rádio). Hoje parece normal fazer cursos on-line, preencher formulários administrativos a distância ou expressar opiniões em fóruns de discussão. Segundo a última pesquisa realizada em 2013 pelo Instituto Brasileiro de Geografia e Estatística (IBGE), mais de 100 milhões de brasileiros estão conectados à internet, e juntamente com iniciativas governamentais de aumentar o acesso da população a internet este número tende a crescer ainda mais.

3 OS CIBERCRIMES.

O aparecimento dos primeiros casos de crimes informáticos data da década de 1960, que nada mais eram que delitos onde o infrator manipulava, sabotava, espionava ou exercia uso abusivo de computadores e sistemas. A partir de 1980, houve um aumento das ações criminosas, que passaram a refletir em, por exemplo, manipulações de caixas bancários, abusos de telecomunicação, pirataria de programa e pornografia infantil. Neste sentido pode-se afirmar que o marco inicial da ilicitude digital foi a rápida difusão dos computadores e da internet na sociedade. (Archick 2002)

A “Convenção de Budapeste” (ou “Convenção sobre a Criminalidade”) foi o primeiro tratado internacional com a finalidade de tipificar os principais crimes cometidos através da Internet e outras redes de computadores. A negociação do tratado teve início em 1997, seguindo uma determinação do Conselho da Europa, que o caráter transnacional de cibercrime somente poderia ser tratado a nível global. A Convenção ao de Budapeste foi aberta para assinatura em novembro de 2001, entrando em vigor em julho de 2004 (Archick 2002, Solagna e Souza 2011). Até 16 de agosto de 2011, 16 (dezesseis) Estados haviam assinado, ratificado ou aderido à Convenção, enquanto mais 31 (trinta e um) Estados a assinaram, mas n˜ ao a ratificaram 5 (Redivo e Monteiro 2009, Gouveia 2007)

Importante para a discussão aqui proposta, é que se faça uma explanação acerca dos cibercrimes, haja vista que é um dos pontos mais discutidos quanto à lei 12.737/12, dado que uma das maiores preocupações com respeito ao diploma legal é o fato de que este apresenta um texto vago no tocante as diversas condutas delitivas que podem ser realizadas através do meio cibernético.

Assim se fará de forma que se analisará desde os primeiros indícios da ilicitude digital até a forma como se encontra atualmente, analisando desde seus agentes e a hierarquia que existe entre eles, e os atos praticados por estes.

3.1 CONCEITO DE CIBERCRIME

Segundo Paulo Lima, esse conceito pode ser entendido como:

> Em verdade, os crimes de computador são, na maior parte das vezes, os crimes comuns cometidos, com o auxílio de um computador podendo os crimes de furto apropriação indébita estelionato ou dano ser cometidos por esse meio com consideráveis prejuízos patrimoniais. Entretanto, há algo além de uma nova ferramenta, de um novo meio, de um novo modus operandi para o cometimento de crimes: estamos também diante de novas condutas não tipificadas. (LIMA, 2005, p. 29)

Assim de uma forma simples podemos definir o cibercrime como o ilícito penal que têm por objeto material os dispositivos informáticos e a própria internet, o que nesse ponto se aponta como uma enorme dificuldade, para a elucidação da prática dos mesmo.

Tal se dá baseado no fato de que se pode cometer qualquer conduta tipificada como cibercrime, sem sequer sair de sua residência e inclusive de forma praticamente anônima.

Ainda no intuito de fortalecer este entendimento pode-se destacar o entendimento de Gustavo Testa Correa, que apresenta o seguinte conceito para o cibercrime:

> "Todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar, para tal prática é indispensável à utilização de um meio eletrônico"

Tal conceito é mister no fato que, no diploma legal em análise nesse trabalho, o legislador pátrio buscou trazer regulamentação legal justamente a invasão de dispositivos informáticos.

3.2 ESPÉCIES DE CRIMINOSOS DIGITAIS.

Verifica-se que é necessário se explanar do que vêm a ser as condutas praticadas pelos criminosos digitais e como estas podem ser classificadas e isso se faz no tocante que a conduta em ambos os agentes nesse tipo de crime pode variar de forma, resultado e meio de execução.

Hacker[3] é o termo mais comum para se referir a aquele que comete algum crime se valendo dos meios informáticos, no entanto tal nomenclatura se demonstra

[3] Em informática, hacker é um indivíduo que se dedica, com intensidade incomum, a conhecer e modificar os aspectos mais internos de dispositivos, programas e redes de computadores. Graças a esses conhecimentos, um hacker frequentemente consegue obter soluções e efeitos extraordinários, que extrapolam os limites do funcionamento "normal" dos sistemas como previstos pelos seus

como sendo errônea, posto que tal termo foi cunhado de forma a discriminar uma única conduta e, que dependendo da análise, não pode nem mesmo ser vista como crime.

Na verdade, existem outros agentes que, pela forma que agem, recebem nomenclaturas diferentes. Dentre eles deve-se citar:

3.2.1 Hacker

É aquela pessoa que possui uma grande facilidade de análise, assimilação, compreensão e capacidades surpreendentes de conseguir fazer o que quiser (literalmente) com um computador. Ela sabe perfeitamente que nenhum sistema é completamente livre de falhas, e sabe onde procurar por elas, utilizando de técnicas das mais variadas. Hackers são necessariamente programadores habilidosos (mas não necessariamente disciplinados). Suas motivações são muito variadas, incluindo curiosidade, necessidade profissional, vaidade, espírito competitivo, patriotismo, ativismo ou mesmo crime. Todavia embora o Hacker análise as falhas que existam em vários sistemas, muitas vezes as faz sem invadir nenhum dispositivo.

Assim sendo nota-se que o termo hacker não mostra adequado ao tipo penal da Lei 12.737/12 de forma que ele pode realizar condutas de forma a nunca invadir qualquer dispositivo informático alheio.

3.2.2 Cracker

É o termo usado para designar o indivíduo que pratica a quebra (ou cracking) de um sistema de segurança, de forma ilegal ou sem ética. Este termo foi criado em 1985 por hackers em defesa contra o uso jornalístico do termo hacker. O uso deste termo reflete a forte revolta destes contra o roubo e vandalismo praticado pelo cracking. Existem duas linhas de Crackers: os de Criptografia: que se dedicam à quebra de criptográfia (cracking codes). Tal procedimento pode ser executado tanto

---

criadores; incluindo, por exemplo, contornar as barreiras que supostamente deveriam impedir o controle de certos sistemas e acesso a certos dados.
O termo (pronunciado "háquer" com "h" espirado) é importado da língua inglesa, e tem sido traduzido por decifrador (embora esta palavra tenha outro sentido bem distinto) ou aportuguesado para ráquer.3 Os verbos "hackear" e "raquear" costumam ser usados para descrever modificações e manipulações não triviais ou não autorizadas em sistemas de computação.

com lápis e papel bem como com uso de computadores, tudo depende da fonte do problema a ser solucionado. Também há os Crackers de softwares, que fazem engenharia reversa de um determinado programa, ou seja, alteram o conteúdo de um determinado programa pra fazer funcionar de forma correta, muitos crackers alteram datas de expiração de um determinado programa pra fazer funcionar mais de 30 dias, ou seja, modificam o modo trial para utilizar como se fosse uma cópia legítima, ou fazem um desvio interno na rotina de registro do programa para que ele passe a aceitar quaisquer seriais, tais softwares alterados são conhecidos como *warez*.

Dentro dessa espécie podemos destacar os desenvolvedores de vírus, *worms*, trojans e outros malwares: programadores que criam pequenos softwares que causam danos ao usuário. Além de instalar backdoors[4], que iram dar a ele controle futuro de uma máquina infectada.

E por tais motivos Cracker é o termo mais apropriado pra se referir ao indivíduo que invade dispositivos informáticos alheios, e cuja conduta foi recentemente tipificada.

Como se pode evidenciar em análise ao artigo 154-A do Código Penal, cuja redação é dada pela Lei 12.737:

> "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:"
>
> § 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"

Assim fica evidente que este tipo, é o que se tinha em mente quando se idealizou essa mudança no Código Penal.

[4] Backdoor (também conhecido por Porta dos fundos) é uma falha de segurança que pode existir em um programa de computador ou sistema operacional, que pode permitir a invasão do sistema por um cracker para que ele possa obter um total controle da máquina (e se o cracker ter o controle da máquina suas informações e arquivos do computador podem ser roubadas). Muitos crackers utilizam-se de um Backdoor para instalar vírus de computador ou outros programas maliciosos, conhecidos como malware.

3.2.3 Phreaker.

É especializado em telefonia. Faz parte de suas principais atividades as ligações gratuitas (tanto local como interurbano e internacional), reprogramação de centrais telefônicas, instalação de escutas (não aquelas colocadas em postes telefônicos, mas imagine algo no sentido de, a cada vez que seu telefone tocar, o dele também o fará, e ele poderá ouvir sua conversa), etc. O conhecimento de um phreaker é essencial para se buscar informações que seriam muito úteis nas mãos de mal-intencionados. Além de permitir que um possível ataque a um sistema tenha como ponto de partida provedores de acesso em outros países, suas técnicas permitem não somente ficar invisível diante de um provável rastreamento, como também forjar o culpado da ligação fraudulenta, fazendo com que o coitado pague o pato (e a conta).

Estes tipos de criminosos são os que mais se amoldam as condutas tipificadas no §1º, art. 266 da Lei 12.737/12, que diz:

> Art. 266 (...).
> "§ 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

Nota-se que suas condutas envolvem a invasão de dispositivo, como também a interrupção serviço telemático ou de informação de utilidade pública, além impede ou dificulta-lhe o restabelecimento, o que embora já demonstre uma certa lacuna do texto legal quanto a interceptação, que muitas vezes envolve a clonagem de uma número telefônico.

3.3 PRINCIPAIS AMEAÇAS VIRTUAIS.

3.3.1Backdoor

Traduzido do inglês como "porta dos fundos", esta técnica é bastante utilizada por cibercriminosos para ganhar acesso a um sistema e infectá-lo, ignorando as defesas do sistema através de uma falha não documentada do sistema operacional, programa ou na rede onde o computador está instalado.

3.3.2 Ladrões de Informação

Neste grupo entram os keyloggers e memory scrapers, malwares desenvolvidos com o objetivo específico de roubar informações pessoais do usuário, como senhas de banco, dados pessoais e informações sigilosas, não fazendo nenhum mal para o sistema.

Os keyloggers basicamente gravam todas as teclas digitadas pelo usuários e enviam para o criminoso sempre que tiver oportunidade. Por exemplo, se nos dados enviados consta o endereço do seu banco, é muito provável que os próximos caracteres serão os dados da conta e senha do cartão.

Os memory scrapers são um pouco mais genéricos, gravando as informações que estão contidas na memória RAM do sistema.

3.3.3 Worms.

Um vírus comum precisa de um programa hospedeiro para se propagar, o worm (ou verme, em português) é um pacote completo auto replicador, sendo projetado para tomar decisões de como quebrar as falhas de segurança de um sistema e agir de forma completamente autônoma, decidindo quando enviar um e-mail com informações importantes para o invasor, por exemplo.

Quando um usuário tem a sua máquina infectada por um worm, qualquer outra que esteja conectada à rede está igualmente vulnerável. Detectá-lo é possível somente através de modos indiretos, como lentidão no PC e na conexão com a internet, ou mesmo com vários programas abrindo ao mesmo tempo sem a interação do usuário.

3.3.4 Ransomware.

Malware que está se tornando bastante comum, o ransomware trava o computador do usuário até que ele pague um resgate para ter o controle de seus dados de volta, e normalmente o valor não é baixo. Com isso, o dono do computador não possui acesso aos seus próprios arquivos, que normalmente ficam encriptados, e a única solução é pagar o valor cobrado para não perder dados importantes.

Alguns podem pensar que basta simplesmente formatar a máquina, mas os principais alvos desse tipo de ataque são pessoas que realmente necessitam preservá-los - já que em muitas máquinas estão armazenadas informações de empresas que, se utilizadas, podem causar inúmeros transtornos. O grande problema é que, em muitas vezes, o invasor não devolve o controle para o usuário mesmo após o pagamento da "taxa".

3.3.5 Trojans de Acesso Remoto (RAT).

Trojans (RAT - Remote Access Trojans) podem ser considerados como uma evolução das backdoors, fornecendo ao invasor uma interface gráfica com várias opções para comprometer o acesso do usuário. Muitos computadores são infectados sem grandes consequências, já que naquele momento não há nada que interesse ao invasor, que só fica monitorando as atividades realizadas.

Quando é detectado algo interessante, como o acesso à rede de uma empresa ou ao site de um banco, o criminoso pode monitorar e capturar os dados descobertos. Em muitos casos, quando o usuário não faz nada de "interessante", o criminoso simplesmente danifica ou mesmo inutiliza a máquina.

3.4 “HACKERS” FAMOSOS.

3.4.1 Kevin Mitnick

Mitnick é o hacker mais famoso do mundo, sendo que em 1990 conseguiu invadir a rede de computadores das operadoras de telefonia e de provedores de internet nos Estados Unidos. Além disso, foi capaz de enganar o FBI diversas vezes chegando a figurar na lista dos cibercriminosos mais procurados do mundo. Preso em 1995 ficou 5 anos atrás das grades saindo após pagar fiança, porém teve que ficar os três primeiros anos soltos sem se conectar. Atualmente, Mitnick trabalha como consultor de segurança digital.

3.4.2 Adrian Lamo

Adrian Lamo nascido em 1981 em Boston, Massachusetts nos Estados Unidos, é um famoso hacker, (grey hat hacker), principalmente conhecido por quebrar uma série de sistemas de alta segurança de rede de computadores, como a Microsoft, a Yahoo!, a MCI WorldCom, a Excite@Home, as empresas de telefonia SBC, Ameritech e Cingular e o New York Times. Foi preso somente após invadir o New York Times.

Normalmente, Adrian apenas invadia sistemas para encontrar falhas e reportá-las ao administrador do sistema. O episódio do New York Times foi diferente pois o NYT já estava com a reputação de sua segurança manchada após serem invadidos pelo grupo hacker "Hacking for girlie". O *hack* de Adrian feriu a moral dos responsáveis pela segurança que havia se dedicado para que o episódio do grupo "Hacking for girlie" não ocorresse novamente.

O grupo "Hacking for girlie" invadiu o NYT criticando o artigo que John Markoff escreveu sobre Kevin Mitnick, que contribuiu para o tratamento duro que Kevin Mitnick recebeu ao ser preso.

3.4.3 Raphael Gray

O hacker britânico Raphael Gray, foi condenado por roubar 23 mil números de cartões de crédito, entre eles um de Bill Gates.

3.4.4 Jonathan James.

Jonathan Joseph James (12 de Dezembro de 1983 – 18 de Maio de 2008) foi um hacker dos Estados Unidos da América, tendo sido a primeira pessoa de idade juvenil a ser encarcerado por cibercrime no seu país.1 Tinha 15 anos aquando do seu primeiro crime e 16 anos quando a sentença foi proferida. Morreu a 18 de Maio de 2008, ao infligir um tiro de arma de fogo em si próprio

3.4.5 Jon Lech Johansen.

Jon Johansen, conhecido como DVD Jon, (Harstad, 18 de novembro de 1983) é um hacker norueguês. Conquistou fama após descobrir como burlar a proteção regional que é inserida nos discos de DVD comerciais. Os DVDs produzidos pela indústria do cinema recebem um código regional que o impede de ser reproduzido fora de sua área de venda, numa tentativa de inibir a falsificação. Os códigos regionais são nove no total.

Posteriormente, Johansen desenvolveu outro programa capaz de violar o dispositivo anti-cópia dos arquivos de áudio da Apple Inc. (AAC).

Em 2005, com apenas 21 anos, Jon foi contratado pela empresa MP3Tunes para um projeto que envolverá a violação de dispositivos de proteção, alegadamente, apenas para desenvolver melhorias, baseado no princípio de engenharia reversa. O dono da MP3Tunes, Michael Robertson, desenvolveu no passado um programa que permite usar o software iTunes com aparelhos de MP3 que não o iPod da Apple.

3.4.6 Vladimir Levin.

O russo Vladimir Levin é o ladrão digital mais notório da história. Ele liderou uma gangue russa que invadiu os computadores do Citibank e desviou US$ 10 milhões de contas de clientes. Levin foi preso na Inglaterra, quando tentava fugir do país. Ele dizia que um dos advogados alocados para defendê-lo era, na verdade, um agente do FBI.

Aqui fica evidente que as práticas desenvolvidas pelos criminosos digitais se apontam como as mais diversas, indo desde fraude bancária, a violação e invasão de dispositivos, como a pirataria e quebras de protocolos de segurança.

3.5 ENGENHARIA SOCIAL, SPAM E PHISHING.

Outro ponto de grande relevância é a conjunção dessas condutas a Engenharia Social, o Spam e o Phishing, não só por ser a prática mais crescente como têm se mostrado uma das mais efetivas no Brasil.

A Engenharia Social consiste em ludibriar ou explorar a confiança de usuários não treinados, para induzi-los a dar acesso a informações sigilosas, se valendo de sua inaptidão, é uma forma de adquirir informações sem realizar qualquer invasão, posto que leva a vítima a fornecê-la, pois esta acredita ser um procedimento correto.

Essa prática, se revela muito presente na atualidade, isso se dá pela grande difusão da informática, e o fato de que muitos usuários embora acessem a internet com frequência não tem real conhecimento de certas práticas e procedimentos.

Tal conduta no meio cibernético, está bem atrelada a figura do *Spam*[5]*,* que é basicamente um e-mail falso que espalha rapidamente e se dissemina, no intuito de atingir o maior número de pessoas possível, e geralmente busca ludibriar usuários ao se passar por bancos, provedores de internet e hospedagem, firmas de advocacia, farmácias, ou até mesmo os próprios provedores de e-mail. Embora por algumas vezes possa ter fim publicitário, no contexto da prática da engenharia social, será utilizada para explorar a confiança do usuário.

O que leva ao terceiro elemento que é o Phishing, derivado do termo em inglês *fishing*, que quer dizer pescar. Esta é uma fraude eletrônica, que têm por objetivo central a obtenção de informações principalmente bancárias, ou até mesmo de identidade com intuito de fazer uso delas.

Neste sentido ao se unir a Engenharia Social, o Spam e o Phishing se identifica uma única conduta com etapas diversas e com inúmeras formas de agir, como no golpe mais comum de roubo de dados de usuário e senha que dão acesso a contas de e-mail.

A conduta se faz da seguinte forma: valendo-se do preceito que grande parte dos usuários não conhece sobre as políticas de envio de e-mail de bancos e outras empresas, o autor da conduta delitiva cria um site falso imitando o de algum banco, e dentro dele insere formulários em que o usuário ao preencher fornece ao criminoso todos os seus dados pessoais, além de no momento da criação do site falso ele já criar também um e-mail que este utilizará para conseguir suas vítimas.

---

[5] O termo spam pode significar Sending and Posting Advertisement in Mass, ou "enviar e postar publicidade em massa", ou também: Stupid Pointless Annoying Messages que significa mensagem rídicula, sem propósito, e irritante. No entanto, existem diversas versões a respeito da origem da palavra spam. A versão mais aceita, e endossada pela RFC 2635, afirma que o termo originou-se da marca SPAM, um tipo de carne suína enlatada da Hormel Foods Corporation, e foi associado ao envio de mensagens não-solicitadas devido a um quadro do grupo de humoristas ingleses Monty Python.

Para alcançar o maior número de usuários possível o criminoso se vale do envio de spams no intuito de poder alcançar mais vítimas, e isso se dá de maneira que, no conteúdo do e-mail falso, pode conter ou uma *URL*[6] falsa que irá direcionar a vítima para o site previamente criado, ou ainda programa que se instale no dispositivo da vítima e capture as informações desta.

Outra ferramenta de engenharia social, muito presente em spams, é se valer de um Hoax, que é um termo da língua inglesa que significa boato, nessa o criminoso pega um fato de grande repercussão, e envia e-mails que se referem a ele no intuito de ludibriar o usuário e leva-lo a abrir o e-mail, no que pode resultar ao direcionamento da vítima ao site falso criado pelo criminoso, ou fará com que seja instalado um programa que irá capturar as informações desta.

3.6 HACKTIVISMO

Todavia esses tipos supramencionados são os mais comuns, e não refletem novas condutas criminosas que surgiram, pois atualmente se vê com maior notoriedade as atividades de Hacktivismo, que são basicamente ataques aos serviços informáticos como forma de protesto e que, vêm se tornando cada vez mais frequentes e mais danosos.

Dentre os principais grupos de Hacktivismo, podemos destacar o LulzSec e Anonymous, que foram os principais militantes, de ideais como a liberdade da internet sem grande regulamentação estatal e de garantias a privacidade mas, para isso fazem ataques a entes governamentais para difundir seu movimento.

Uma das principais ações dos grupos de Hacktivismo são os ataques de *DDoS*, um ataque de negação de serviço (também conhecido como DoS Attack, um acrônimo em inglês para Denial of Service), é uma tentativa em tornar os recursos de um sistema indisponíveis para seus utilizadores. Não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga que consiste em um gigantesco fluxo num curto espaço de tempo de acessos algum site, de forma que o servidor que o hospede não posso administrar o grande fluxo de acessos e acabe por deixar de funcionar tornando o site agora inacessível.

---

[6] Um URL (de Uniform Resource Locator), em português Localizador-Padrão de Recursos, é o endereço de um recurso (como um arquivo, uma impressora etc.), disponível em uma rede; seja a Internet, ou mesmo uma rede corporativa como uma intranet.

3.7 OS CIBERCRIMES NO BRASIL E COMO ESTES SÃO COMBATIDOS.

Nas palavras de Rogério Greco (2013), “A Internet supõe um sonho para seus usuários e um pesadelo para os práticos do direito. Por uma parte, permite concluir transações com empresas e consumidores situados em qualquer lugar do planeta, agiliza a comunicação entre as pessoas. Representa a liberdade mundial de informação e da comunicação; é um sonho transformado em realidade.”

Por outro lado, todo conjunto de atividades sociais precisa de regulamentação. As legislações nacionais avançam com muito atraso no que diz respeito às novas tecnologias. Isso faz com que sejam dificultadas as respostas legais a numerosos litígios que podem suscitar as operações na internet. Por isso é também um pesadelo jurídico.

Um espanhol, usuário da internet, pode acessar a rede e contatar com uma empresa alemã, vendedora ou prestadora de serviços, graças ao acesso à internet, proporcionado pela filial holandesa de um provedor norte-americano. As fronteiras estatais se diluem na internet. A aldeia global se transformou em realidade.

Pode-se dizer que as questões legais mais espinhosas, as quais são colocadas no ciberespaço, correspondem ao direito internacional privado.

Assim sendo, fica evidente já aqui aquela que é tida como a maior celeuma em relação aos cibercrimes, que é o local da infração, pois na atualidade são cada vez mais comuns ferramentas que asseguram ao usuário anonimato de suas atividades na internet, o que dificulta a prevenção e principalmente ao combate as atividades criminosas nos meios informáticos.

No Brasil já existem órgãos com a finalidade de combater ao cibercrime, sendo eles: a Delegacia de Polícia Civil - Divisão de Repressão aos Crimes de Alta Tecnologia (DICAT) que se localiza no Distrito Federal, a Delegacia de Polícia Civil - Delegacia de Repressão a Crimes Eletrônicos localizada no Espírito Santo, a Delegacia de Polícia Civil - Setor de Análise da Gerência de Inteligência da Polícia Civil - Goiânia localizada em Goiás, a Delegacia de Polícia Civil De MS - Delegacia Virtual de MS localizada no Mato Grosso do Sul, a DEICC - Delegacia Especializada de Investigações de Crimes Cibernéticos localizada em Minas Gerais, a Delegacia de Polícia Civil - Delegacia Virtual localizada no Pará, a Delegacia de Polícia Civil - Núcleo de Combate aos Cibercrimes (Nuciber) localizada no Paraná, a Delegacia de

Polícia Civil - Delegacia de Repressão aos Crimes de Informática (DRCI) localizada no Rio de Janeiro, a Delegacia de Repressão aos Crimes Informáticos (DRCI) junto ao Departamento Estadual de Investigações Criminais (DEIC) localizada no Rio Grande do Sul e a Polícia Civil - 4ª Delegacia de Delitos Cometidos por Meios Eletrônicos – DIG/DEIC localizada em São Paulo. (Safernet, 2014)

No entanto, ainda se nota que existem apenas 11 delegacias responsáveis pela investigação de cibercrimes, ou seja, não se chega nem a metade dos estados que formam o país. Todavia, ainda que hajam diversas delegacias focadas no combate ao cibercrime, a investigação do mesmo se encontra extremamente deficiente, conforme as palavras de Emerson Wendet, Delegado Da Polícia Civil do Rio Grande do Sul, em palestra ministrada na sétima edição do seminário segurança da Informação (Seginfo), realizada no Rio de Janeiro, de 30/08 a 01/09.

Segundo ele, uma grande barreira a investigação do cibercrime é o de apurar a prática delituosa, dado onde ocorre o crime. Tal é fator primordial para se proceder na investigação de prática de algum crime, e que se faz dificultada no tocante aos cibercrimes.

Quanto ao local da prática do crime temos entendimento de CAPEZ (2013):

> "Lugar do crime é tanto o da conduta quanto o do resultado. Será, portanto, o lugar onde se deu qualquer dos momentos do iter criminis"

No caso da invasão de dispositivos, integrar os membros participantes da investigação é essencial, posto que pode ocorrer a situação em que um indivíduo no Amazonas invada um dispositivo no Rio Grande do Sul, haveria uma séria barreira para apurar a autoria da invasão, dado que pelo local tanto do autor como da vítima estão separados geograficamente por uma larga distância. Situação essa inclusive, que demonstra ser a mais comum.

Neste sentido, pelo fato de não ocorrer uma integralidade entre os estados, ou até mesmo a criação de Banco de Dados Central, que reúna informações disponíveis a todos os estados, a investigação fica prejudicada já em sua primeira fase.

Outro ponto importante abordado foi a questão da falta de especialização, que embora haja profissionais para investigar os cibercrimes, este não possuem especialização para tal, além de inclusive não possuírem softwares necessários para a realização da investigação e da coleta de provas.

Esta dificuldade, se revela preocupante no sentido que o cibercrime evolui em paralelo com a tecnologia e se os agentes competentes para combate-lo ficarem sempre um passo atrás, perderão todo o seu poder de agir no combate as práticas criminosas no meio cibernético.

3.7.1 A Lei nº 12.735 de 30 de Novembro de 2012.

Juntamente com a lei 12.737/12 foi a aprovado também este diploma legal que, embora durante sua edição tenha sofrido diversas alterações trouxe uma importante mudança quanto a investigação do cibercrime.

A lei trouxe a seguinte mudança em seu texto:

> "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."

Embora, o texto possa parecer redundante ao passo que trata da estruturação de setores especializado no combate aos crimes praticados em rede de computadores bem como dispositivos informáticos e sistemas informatizados.

Sua importância se dá que ao ser regulada na forma da Lei as ações de criar a regulamentar tais setores ganhou uma força adicional, força essa necessária dado ao déficit estrutural que os setores da polícia que investiga o cibercrime enfrenta.

4 A LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.

Sistemas informáticos fazem parte do dia-a-dia de todos os cidadãos na sociedade da informação, hoje não se pode mais prescindir da tecnologia da informação, estando ela configurada nas mais diversas formas em nosso cotidiano, seja como um computador desktop, um notebook, um tablet, um pendrive ou até mesmo um GPS, e ainda se estendendo a questão como a de hospedagem ou a de servidor de dados, a todo mundo se está depositando informações e dados dentro de dispositivos e sistemas informáticos.

A partir do fato de que esses sistemas passaram a fazer parte do cotidiano da sociedade, a legislação passará a se preocupar com esses dispositivos e sistemas no intuito de proteger a integridade não só dos dispositivos mas das informações por eles tratadas.

Foi a partir desta preocupação que o legislador elaborou a lei nº 12.737/12, que criou a figura típica da invasão de dispositivos informáticos.

Oriunda do Projeto de Lei 2793/2011, apelidado de “Lei Carolina Dieckmann”, que foi criado em função do caso em que a atriz que deu nome ao projeto, teve vazadas na internet fotos em que aparecia nua. Fator esse que trouxe grande repercussão ao projeto fazendo com este fosse aprovado em tempo recorde.

Todavia, isento do que a lei tenha sido chamada ela trouxe consigo a função de tratar na verdade da invasão de dispositivos informáticos, e o fez ao criar a figura típica do art. 154-A do Código penal, além de trazer mudanças a outros artigos.

Primeiramente segue o texto da lei na integra:

> “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."

Nota-se que, numa análise inicial, esta lei veio com intuito de adequar a legislação, alterando o código penal a fim de tipificar condutas novas que embora fosse outros tipificadas, agora se demonstram mais atualizadas.

Entretanto a maior inovação foi a criação da figura do art. 154-A, junto com o disposto nos §§ 1 à 4, posto que ela veio disciplinando a invasão de dispositivo bem como buscou tipificar também a conduta de quem auxilia na invasão como também trouxe uma forma qualificada da conduta, ao se analisar a finalidade da invasão.

Em suma, tendo em vista o título em que o artigo foi inserido pode-se dizer que ele veio tutelar a liberdade individual de manter dados íntegros em dispositivos informáticos, que possuam medidas de segurança, protegendo o de invasões 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.

Assim sendo, neste trabalho se focará mais na conduta da invasão de dispositivos por se tratar do ponto mais importante tanto pelos direitos que veio tutelar, como por se tratar de uma figura nova no direito pátrio.

4.1 SUJEITOS NO CRIME DE INVASÃO DE DISPOSITIVOS.

O sujeito ativo no crime de invasão de dispositivo pode ser qualquer um, o tipo penal não exige qualquer circunstância pessoal específica, desde que não possua credenciais de acesso ao dispositivo, assim sendo caso um indivíduo mesmo que destrua, adultere ou obtenha dados presentes em um dispositivo informático, desde que possua as credenciais de acesso a este, não comete o crime do art. 154-A do Código Penal.

Já o sujeito passivo, podemos enquadrar duas pessoas sendo a primeira o titular do dispositivo informático, assim sendo, aquele que terá legitimidade para ingressar com representação perante o Ministério Público será aquele que possui o dispositivo invadido, outra hipótese envolve casos de hospedagem, em que uma pessoa é titular do dispositivo informático e outra é a titular dos dados que estão armazenados no dispositivo, em caso de invasão do dispositivo, caso não houvesse desejo do titular do dispositivo de representar contra o invasor, o titular dos dados

poderia fazê-lo já que ele foi o real prejudicado no caso em tela, tal hipótese se faz baseado nas dinâmicas de informação que estão presentes no momento.

4.2 TIPICIDADE.

O tipo legal trata-se de uma das postulações básicas do princípio da reserva legal, que leciona que não há crime sem lei anterior que o defina. Nem pena sem prévia cominação legal, consagrado no art. 5º, XXXIX da Constituição Federal, assim sendo com base neste princípio basilar fica definido que cabe a lei a tarefa de descrever os crimes, assim não cabe à lei penal a tarefa de proibir de forma genérica os delitos, mas sim, o de descrevê-los de forma detalhada, o fazendo de formar a delimitar precisamente o que o ordenamento jurídico entende por fato criminoso.

4.2.1 Tipo Subjetivo.

Conforme leciona CAPEZ (2013) “No elemento subjetivo do tipo, o legislador destaca uma parte do dolo e a insere expressamente no tipo penal. Essa parte é a finalidade especial, a qual pode ou não estar presente na intenção do autor. Quando o tipo incrimi-nador contiver elemento subjetivo, será necessário que o agente, além da vontade de realizar o núcleo da conduta (o verbo), tenha também a finalidade especial descrita explicitamente no modelo legal”.

Posto isso pode-se extrair que no caso dos crimes de invasão de dispositivos informáticos o tipo subjetivo é informado pelo dolo, aqui não cabendo em se falar em figura culposa, e este dolo é específico no sentido que a lei exige que a violação de dispositivo se dê com o fim especial de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita, e aqui cabe-se notar que ficam expostas duas especificidades independentes para o dolo, uma sendo a de instalar vulnerabilidades com intuito de obter vantagem ilícita, não tendo sido definida qual seria tal vantagem, demonstrando aqui a vontade do legislador de que tal vantagem fosse definida em análise ao caso concreto.

Outra especificidade do tipo vêm do obter, adulterar ou destruir dados ou informações, essa é uma especificidade única posto que não exige que tais

condutas tenham como pretensão obter vantagem ilícita, assim não se requer do agente outra vontade a não ser a de simplesmente devassar um sistema e seus dados, apenas como o intuito de bisbilhotar ou por curiosidade apenas.

4.2.2 Tipo Objetivo.

O tipo objetivo se refere ao aspecto material de uma fato, existe no mundo dos fatos e basta que sejam descritos pela norma. São elementos objetivos: o objeto do crime, o lugar, o tempo, os meios empregados, o núcleo do tipo (verbo) etc.

Entretanto o crime previsto no art. 154-A apresenta dois núcleos, os verbos invadir e instalar, inclusive ressalte-se que o tipo penal não exige que o dispositivo esteja ligado seja a internet ou uma intranet.

Essa invasão seguindo o disposto na lei deve ser em dispositivo alheio e mediante violação de mecanismo de segurança, cabendo aqui apontar que este constituem os elementos normativos desta figura típica.

O objeto material do tipo são os dispositivos informáticos alheios, dentre eles podemos compreender vários objetos como desktops, celulares, tablets, smartphones sendo estes pertencentes a pessoa física ou jurídica.

4.3 CONSUMAÇÃO E POSSIBILIDADE DA FORMA TENTADA E DA MODALIDADE CULPOSA.

É essencial que também se faça análise se é possível a existência das formas tentada e culpa nos cibercrimes, dando um enfoque principal a invasão de dispositivos informáticos, regulada pela lei 12.737/12 que é o diploma legal que busca prevenir a maioria das condutas tidas como cibercrimes, no tocante a proteger os dados pessoais do indivíduo, pois conforme se análise a principal mudança que o texto legal trouxe foi o acréscimo do art. 154-A, que foi inserido no rol dos crimes contra a liberdade individual e mais precisamente, nos crimes contra a inviolabilidade dos segredos.

Quanto a consumação essa se dará pela mera invasão cabendo apenas se delimitar para qual especificidade o fez para fins de se atuar seguindo o devido processo legal.

No tocante a forma tentada, seguindo o disposto do art.14, inciso II do Código Penal Brasileiro, em que se considera como crime tentado, aquela que iniciada a execução não se consuma por vontade alheia do agente.

Assim sendo é plenamente aceitável a forma tentada da figura típica, principalmente na invasão de dispositivo, bastando que o agente que deseja praticar o ilícito inicia a execução e por fator independente de sua vontade não se concretize, tal se dará na forma de que, determinado deseja invadir um computador mas, no momento da invasão acaba por ter essa frustrada por ter sido desligado o servidor que este desejava acessar, ou mesmo por ter seu acesso bloqueado por uma firewall[7].

Já em outro sentido não pode ser aceita a forma culposa, pois ao se seguir o mesmo entendimento em análise a conduta típica, esta inexiste, seguindo o que dispões o art. 18, inciso II do Código penal que define como crime culposo quando, o agente deu causa ao resultado por imprudência, negligência ou imperícia, tão logo se lê o texto da lei fica evidente que inexiste a forma culposa do crime de invasão posto que ainda que ao se analisar o núcleo do tipo penal, este tipifica a conduta como invadir e indica que, essa se fará com intuito de adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

4.4 CONDUTAS EQUIPARADAS

No §2º do art. 154-A o legislador trouxe uma outra figura e equiparou a sua conduta com a de quem prática o ilícito do *caput* do artigo, que foi a de quem oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

Assim sendo ficariam impostas as mesmas penas de quem invade um determinado dispositivo alheio, aos indivíduos que fornecem as ferramentas para que estes o façam. De toda forma tal conduta pode ser vista sob dois primas, uma que é a de penalizar os indivíduos que fomentam as atividades de invasão a dispositivos informáticos, a outra forma de analisar é que podem desta tipificação

[7]É um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede. O firewall pode ser do tipo filtros de pacotes, proxy de aplicações, etc.

surgir a problemática de que uma pessoa que criou um programa com função diversa, teve este pervertido para invadir um dispositivo.

4.5 CAUSAS DE AUMENTO DE PENA.

Já no §2º do art. 154-a, o legislador elencou uma causa de aumento de pena que é a de aumentar-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico, figura que se demonstra bem clara, posto que o legislador aqui se demonstrou preocupado em punir com mais gravidade o prejuízo econômico que por ventura poderia advir da invasão do dispositivo.

Tal figura se mostrou bem clara demonstrada que só irá ser aumentada a pena se houve prejuízo econômico não cabendo se falar em outros prejuízos como uma possível dano moral que possa ocorrer.

Outra hipótese de aumento de pena foi elencada no §5º do art. 154-A:

> "§ 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."

Tal cláusula de aumento de pena se faz presente pelo fato de que não só se dirige a tipificar de forma mais gravosa a invasão de dispositivos informáticos pertencentes aos agentes da administração estatal, como também aos dados dos quais esses dispõe e processam em seus dispositivos.

4.6 FORMA QUALIFICADA.

Quanto à forma qualificada do crime de invasão de dispositivos informáticos o legislador elencou no §3º do art. 154-A, as seguintes hipóteses:

Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, nessa figura o legislador buscou abranger de forma genérica as várias formas de comunicação que possuímos, que vai desde e-mails até mensagens de textos.

Os segredos comerciais ou industriais, de forma a proteger dados que são de grande valia e que por ventura estão armazenados em um determinado dispositivo, o legislador deu enfoque aos segredos comerciais e aos segredos pertencentes as indústrias de forma que estes são bens cuja divulgação pode acarretar prejuízos enormes a seus retentores.

As informações sigilosas, assim definidas em lei, aqui se tratam de informações protegidas por sigilo legal e naturalmente ligadas a órgãos governamentais, inclusive por questões de segurança nacional. Essa figura é uma "norma penal em branco imprópria ou homogênea", pois que exige para seu complemento e aplicabilidade o recurso a outra lei que defina quais são as informações consideradas sigilosas

O controle remoto não autorizado do dispositivo invadido caso em que a invasão enseje o "controle remoto não autorizado do dispositivo" violado. Aqui se tratou basicamente do "acesso remoto" que pode ser feito em determinado dispositivo, podendo inclusive ser implantado de forma legal em empresas, como no caso de programas como o "Team Viewer", são programas como ele que permitem total acesso a uma máquina sendo possível até de se visualizar em tempo real o que está sendo. No entanto a implantação de tais programas pode ser feita também de forma clandestina por meio de trojans ou vírus que podem justamente dar controle total de um dispositivo, e foi justamente com a intenção de tipificar a conduta clandestina de controle remoto de dispositivos que o legislador descreveu tal conduta.

4.7 CRÍTICAS FEITAS AO TIPO PENAL CRIADO PELA LEI 12.737/12.

O núcleo do tipo penal de invasão de dispositivos se encontra no termo "invadir", pressupondo a entrada forçada em determinado dispositivo, ou como escrito no próprio texto do diploma legal, violando de forma indevida mecanismo de segurança, cabe aqui dar ênfase ao termo "alheio" presente no tipo, haja vista que não se poderá invadir dispositivo que não seja alheio.

Ao se observar a conduta típica do artigo desde já podemos classificar o crime do art.154-A como sendo um crime formal.Pois seguindo entendimento de CAPEZ (2013) que ao classificar o crime formal disse:

> "O tipo não exige a produção do resultado para a consumação do crime, embora seja possível a sua ocorrência. Assim, o resultado naturalístico,

> embora possível, é irrelevante para que a infração penal se consume. É o caso, por exemplo, da ameaça, em que o agente visa intimidar a vítima, mas essa intimidação é irrelevante para a consumação do crime, ou, ainda, da extorsão mediante sequestro, no qual o recebimento do resgate exigido é irrelevante para a plena realização do tipo. Nesses tipos, pode haver uma incongruência entre o fim visado pelo agente — respectivamente, a intimidação do ameaçado e o recebimento do resgate — e o resultado que o tipo exige. A lei exige menos do que a intenção do sujeito ativo (v. g., ele quer receber o resgate, mas o tipo se contenta com menos para a consumação da extorsão mediante sequestro). Por essa razão, esses tipos são denominados incongruentes"

Posto isto é certa a classificação, dado que embora possa advir o resultado, em que haja a divulgação dos dados, a exploração econômica dos dados, ou até mesmo algum de pedido de resgate pela devolução dos dados obtidos, para que haja o enquadramento na figura típica do art. 154-A basta que haja a invasão, ou seja não exige um resultado para que se tenha a consumação do crime.

Outra expressão presente no art.154-A que precisa ser analisada foi que o legislador, fez uso do seguinte termo ou como escrito no próprio texto do diploma legal, "violando de forma indevida mecanismo de segurança", aqui fica estabelecido que só pode ser tipificada a invasão de dispositivo que possua mecanismo de segurança, ou seja, se por uma acaso um indivíduo invade determinando dispositivo que esteja desprovido de mecanismos de segurança, acaba por não cometer crime algum.

Esse tópico acabou por se tornar o mais preocupante, dado que o legislador não definiu o que propriamente seriam mecanismos de segurança, assim sendo ao imaginarmos a seguinte situação:

O indivíduo A invade dispositivo informático pertencente a um indivíduo B, o dispositivo antes possuía mecanismos de segurança, como antivírus ou uma firewall, no entanto o indivíduo B acaba baixando um trojan que desabilite os mecanismos de segurança que este, no momento que o indivíduo A tentar invadir o dispositivo informático pertencente a B, este não cometerá crime algum visto que o dispositivo se encontrava plenamente aberto, e isto independente do que o indivíduo A objetive fazer com os dados que obteve.

E no caso do exemplo acima, podemos apontar aqui um desleixe do legislador ao editar o diploma legal, pois não pode prever tal hipótese cuja ocorrência pode ser bastante corriqueira.

Outra expressão do diploma legal que merece análise é quando o legislador diz “instalar vulnerabilidades para obter vantagem ilícita”, primeiro do ponto de vista técnico não existe a possibilidade de se instalar uma vulnerabilidade em qualquer dispositivo informático, acredita-se aqui que os editores do dispositivo legal, tinha em mente a questão dos *backdoor’s*, que deixam o sistema aberto para uma futura infecção por programas maliciosos.

Contudo, o *backdoor,* não é instalado no dispositivo, como já foi anteriormente descrito, este procedimento se fez ignorando as defesas do sistema através de uma falha não documentada do sistema operacional.

Diante disso, diante de um caso em que um indivíduo apenas explore uma vulnerabilidade do sistema sem ter que proceder com a instalação de qualquer programa que venha a tornar o dispositivo mais vulnerável ele não comete crime algum.

Mais um ponto importante do texto é quando o dispositivo legal trouxe o seguinte “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”.

Desta forma o legislador elencou a hipótese em se pode invadir determinado dispositivo informático alheio, mesmo com o objetivo de obter, adulterar ou até mesmo de destruir informação, e que tal não se configurará como crime desde que haja a autorização expressa, e essa seria como no caso de uma empresa que contratou um professional para analisar a segurança de seus dispositivos e que para isso tentará invadi-los mas, trouxe também a figura da autorização tácita.

É justamente com a figura tácita da autorização de invasão de dispositivo que se deve tomar cuidado, pois o legislador embora a tenha elencado não a descreveu, deixando vaga como se daria essa autorização, e aqui se gerou uma problemática ao fato de que no caso concreto caso haja a invasão, de dispositivo alheio sendo esta mediante violação de mecanismo de segurança e que tenha destruído dados, se este indivíduo que deseja invadir o dispositivo pediu por autorização e dado certo tempo não houve negativa, esta não poderia ser considerada crime.

Posto isto o problema que surge é qual seria o lapso temporal necessário para se entender que foi autorizada a invasão de determinado dispositivo, posto que deve-se levar em conta o fato de que nos dias de hoje a comunicação se tornou

extremamente mais dinâmica, contudo ainda deve-se levar em conta o fator humano da equação, sendo este fator suscetível a retardar essa comunicação.

Ante o exposto fica evidente que tais lacunas se demonstram prejudiciais para os aplicadores do Direito pois, implicam em uma análise mais aprofundada do tipo penal de forma que este agora terá que se limitar a um rol bem restrito de situações fáticas.

5 CONSIDERAÇÕES FINAIS.

A análise efetuada acerca do tema proposto no presente trabalho, sem a pretensão de exaurir o assunto abordado, resultou nas considerações a seguir delineadas.

Por muito tempo se falou em se criar leis que viessem a regular os crimes cometidos no meio cibernético e que envolvessem a invasão de dispositivos dentre outras condutas.

A tendência a se seguir pelo Estado é a de editar e aplicar leis que venham a tipificar os delitos informáticos, no intuito de proteger toda uma nova gama de bens jurídicos que agora surgiram junto com o entrelaçamento dos dispositivos informáticos em nossa sociedade.

E seguindo esta tendência o legislador brasileiro buscou elaborar inúmeros projetos de lei com intuito de se tipificar as condutas tidas como crimes envolvendo dispositivos informáticos, desse esforço do legislador surgiu o PL 2793/2011, que mais tarde foi aprovado e deu origem a Lei nº 12.737/12, dispositivo legal que trouxe duas enormes inovações para o Direito brasileiro.

A primeira grande inovação foi a que justamente foi a primeira lei a tipificar especificamente o crime de invasão de dispositivo informático, criando o art.154-A do Código Penal.

A segunda grande inovação foi por se tratar da primeira lei que veio realmente a tipificar uma conduta relacionada ao cibercrime, posto que se tinha um déficit de uma legislação especifica voltada para este tema.

Contudo verificou-se que existiram certos problemas quanto ao texto do diploma legal, principalmente por envolver certas situações relacionadas à informática que apresenta relações diferenciadas e que acontecem num plano diferenciado, que é o da internet e dos dispositivos informáticos.

E justamente após uma análise técnica da redação que a Lei 12.737/12 trouxe, ficou evidenciado que existiam uma série de problemas que poderiam advir da interpretação da norma e das situações que ela veio a tipificar.

Um dos problemas se baseia que um dos princípios norteadores da lei penal é o princípio da reserva legal, e preceitua que nenhuma conduta será tida como crime a não ser que tenha lei anterior que a caracterize como tal. Assim sendo para uma lei que buscou regular os cibercrimes, e haja vista que estes podem se

apresentar sob inúmeras faces além da invasão de dispositivo, deixar de descrever várias condutas que se enquadrem como prejudiciais ao bem tutelado, que no caso dos crimes informáticos, são os dados que estes podem possuir, e justamente por esta falta de previsão legal que surgiram diversas críticas a Lei. 12.737/12.

Desse modo, diante da situação exposta, em face de princípios como o da reserva legal que exige que a conduta definida como crime seja descrita no texto legal, o da proibição da analogia “in malam partem” que não permite que haja a adequação típica por semelhança, chegou-se à conclusão de que, embora a Lei 12.737/12 tenha trago consigo a criação de figuras típicas necessárias, deve-se reformular o texto legal, de forma a incluir as demais possibilidades, além de que seja feita uma nova redação com maior teor técnico que abranja as situações que existem no mundo cibernético, além claro de que esta por buscar regular crimes ligados a tecnologia se mantenha em constante atualização.

REFERÊNCIAS

BORGES, Abimael. **Lei Carolina Dieckmann - Lei nº. 12.737/12, art. 154-a do Código Penal.** Disponível em: < http://abimaelborges.jusbrasil.com.br/artigos/111823710/lei-carolinadieckmann-lei-n-12737-12-art-154-a-do-codigo-penal> acesso em: 20 de fevereiro de 2014.

BRASIL. Lei Nº 12.735, De 30 De Novembro De 2012. Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Brasília, 30 de novembro de 2012; 191º da Independência e 124º da República

_____. 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. Brasília, 30 de novembro de 2012; 191º da Independência e 124º da República

_____. Constituição Federal de 05 de outubro de 1988. In**: Vade Mecum**. Obra coletiva da Editora Saraiva**,** com a colaboração de Antônio Luiz de Toledo Pinto, Maria Cristina Vaz dos Santos Windt e Lívia Céspedes. 9 ed. atual. e ampl. São Paulo: Saraiva, 2013.

_____. Decreto-Lei no 2.848, de 7 de dezembro de 1940. Código Penal. In**: Vade Mecum.** Obra coletiva da Editora Saraiva**,** com a colaboração de Antônio Luiz de Toledo Pinto, Maria Cristina Vaz dos Santos Windt e Lívia Céspedes. 9 ed. atual. e ampl. São Paulo: Saraiva, 2013.

CABETTE, Eduardo Luiz Santos**. Primeiras impressões sobre a Lei nº 12.737/12 e o crime de invasão de dispositivo informático.** Jus Navigandi, Teresina, ano 18, n. 3493, 23 jan. 2013. Disponível em: <http://jus.com.br/artigos/23522>. Acesso em: 22 de fevereiro de 2014.

CAPEZ, Fernando. **Curso de direito penal, volume 1, parte geral**: (arts. 1º a 120) / Fernando Capez. — 16. ed. — São Paulo: Saraiva, 2012.1. Direito penal I. Título.

CAVALCANTE, Márcio André Lopes. **Primeiros comentários à Lei n.º 12.737/2012, que tipifica a invasão de dispositivo informático**. Disponível em: <http://www.dizerodireito.com.br>. Acesso em: 18 de fevereiro de 2014.

CIPOLI, Daniel. **Vírus, keylogger, worms, trojans e outros: conheça os diferentes tipos de Malware.** Disponível em: < http://canaltech.com.br/tutorial/seguranca/Virus-keylogger-worms-trojans-e-outros-Conheca-os-diferentes-tipo-de-malware/> acesso em: 20 de fevereiro de 2014.

COIMBRA, Rodrigo. **A Hierarquia Hacker.** Disponível em: < http://projetoseti.com.br/a-hierarquia-hacker/> acesso em: 20 de fevereiro de 2014.

FONSECA FILHO, Cléuzio. **História da computação [recurso eletrônico]: O Caminho do Pensamento e da Tecnologia** / Cléuzio Fonseca Filho. – Porto Alegre. EDIPUCRS, 2007. 205 p.

GLATZL, Rafael da Silva. **A dinâmica tecnológica e o direito à privacidade: reflexões acerca da lei 12.737/12**. Boletim Jurídico, Uberaba/MG, a. 5, no 1113. Disponível em: <http://www.boletimjuridico.com.br/doutrina/texto.asp?id=2843 > Acesso em: 24 fevereiro de 2014.

GOMES, Luiz Flávio. **A (in)eficácia da Lei Carolina Dieckmann.** Disponível em: <http://congressoemfoco.uol.com.br/noticias/a-ineficacia-da-lei-carolina-dieckmann /> acesso em: 28 de setembro de 2013.

JÚNIORM, Sávio. **Constituição e garantia do direito à privacidade dos usuários da Internet.** Disponível em: <http://www.savio.com.br/2009/12/constituicao-e-garantia-do-direito.html> acesso em: 27 de setembro de 2013.

KOCH, Daniel. "**HowStuffWorks - Como funciona a cabeça de um hacker**". Disponível em: < http://informatica.hsw.uol.com.br/cabeca-de-hacker5.htm> acesso em 20 de fevereiro de 2014.

MENEZES, Tyndaro; Soares, Paulo R. **Polícia encontra hackers que roubaram fotos de Carolina Dieckmann**. Fantástico. Disponível em: <http://g1.globo.com/fantastico/noticia/2012/05/policia-encontra-hackers-que-roubaram-fotos-de-carolina-dieckmann.html>. Acesso em: 20 de fevereiro de 2014.

MIRABETE, Júlio F, FABBRINI, Renato N. **Manual de Direito Penal**: parte geral, arts. 1º a 120 do CP. V. 1. 26 ed. Ver. e atual. São Paulo: Atlas, 2010.

MIRANDA, Murilo. **Da persecução penal dos crimes virtuais**. Jus Way: sistema educacional online. Publicado em 27 de janeiro de 2013. Disponível em: <

http://www.jurisway.org.br/v2/dhall.asp? id_dh=9903>. Acesso em: 17 de fevereiro 2014.

NADER, Paulo. **Introdução ao estudo do Direito.** 21ª ed. Rio de Janeiro. Forense, 2001.

NUCCI**,** Guilherme de Sousa. **Manual de direito penal:** parte geral: parte especial. 7ª ed. Editora Revista dos Tribunais, 2011. São Paulo.

SAFERNET. **Delegacias Criminais.** Disponível em: <http://www.safernet.org.br/site/prevencao/orientacao/delegacias> acesso em 22 de fevereiro de 2014.

VENÂNCIA, Pedro Dias. **A previsão constitucional da utilização da Informática.** Disponível em: <http://www.scielo.oces.mctes.pt/scielo.php?pid=S1645-99112007000200012&script=sci_arttext> acesso em: 27 de setembro de 2013.

WIKIPEDIA. **História da computação.** Disponível em: < http://pt.wikipedia.org/wiki/Hist%C3%B3ria_da_computa%C3%A7%C3%A3o> acesso em: 20 de fevereiro de 2014.

_____. **História da Internet**. Disponível em: < http://pt.wikipedia.org/wiki/Hist%C3%B3ria_da_Internet > acesso em: 20 de fevereiro de 2014.

ZAPAROLLI, Rodrigo Alves**. Comentários à Lei nº 12.737/12.** Disponível em: < http://www.jurisway.org.br/v2/dhall.asp?id_dh=10576> acesso em: 24 de fevereiro de 2014.