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

FELIPE GONÇALVES DE MELO

DISCUSSÃO ACERCA DA APLICABILIDADE DA LEI 12.737/2012 EM RELAÇÃO AOS NOVOS CRIMES DE NATUREZA VIRTUAL

SOUSA
2013

FELIPE GONÇALVES DE MELO

DISCUSSÃO ACERCA DA APLICABILIDADE DA LEI 12.737/2012 EM RELAÇÃO AOS NOVOS CRIMES DE NATUREZA VIRTUAL

Projeto de pesquisa 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(a): Prof. Leonardo Figueiredo

SOUSA
2013

FELIPE GONÇALVES DE MELO

DISCUSSÃO ACERCA DA APLICABILIDADE DA LEI 12.737/2012 EM RELAÇÃO AOS NOVOS CRIMES DE NATUREZA VIRTUAL

Projeto de pesquisa 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(a): Prof. Leonardo Figueiredo

Banca Examinadora: Data de Aprovação:____/____/_____

_____

Leonardo Figueiredo

Orientador

_____

Examinador

_____

Examinador

Dedico este trabalho a minha toda minha família,
sobretudo, ao meu saudoso e querido pai,
que infelizmente, no início deste ano,
nos deixou, e também à minha
linda e querida mãe

AGRADECIMENTO

Agradeço a todos aqueles que acreditaram na minha vitória, principalmente minha querida família que nos momentos de desânimo e insatisfação com curso, o qual eu aprendi a gostar, sempre me motivou a terminá-lo.

Ao meu saudoso e eterno pai, Francisco Crispim de Melo, que hoje me vem a mente as palavras que tanto proferia, “meu futuro doutor”, “futuro ministro do STF”, muito em sua função é que estou a galgar os últimos passos dessa quase interminável jornada. Devido ao senhor, me sinto forte o suficiente cada vez mais intensificar os estudos e realizar os objetivos que tanto almejo.

A minha mãe, Marisa Gonçalves de Melo, pois se estou hoje aqui também é em razão da sua incansável orientação e cobrança para que eu sempre me dedicasse, cada vez mais, nos estudos.

Aos meus irmãos Fabíola e Fábio, que mesmo estando longe sempre me deram força para vencer esta batalha.

A todos os meus familiares, que através das boas energias que me passaram, também fazem parte dessa história.

A todos os meus amigos, sobretudo os do Curso de Direito, devido aos inúmeros bons momentos que vivenciamos.

Ao professor orientador, Leonardo Figueiredo, que mesmo com inúmeros compromissos diários, reservou um tempo para corrigir este inacabável e cansativo estudo.

RESUMO

O mundo tem passado por diversas transformações, em compasso com essas mudanças a tecnologia tem evoluído cada vez mais, a partir daí, surgiram diversos dispositivos tecnológicos, os quais proporcionaram comodidade aos usuários, com a prestação dos mais variados serviços. No entanto, apesar de ter trazido diversos benefícios, alguns indivíduos aproveitam-se para o cometimento de crimes, invadindo dispositivos informáticos e violando a privacidade. A sociedade, cada vez mais está interagindo com os meios informáticos, e nessa seara, tem aumentado o número de crimes praticados através dos dispositivos. O caso da atriz Carolina Dieckman, que foi vítima de uma invasão do seu dispositivo informático, onde foram obtidas fotografias íntimas, teve repercussão nacional, e, a partir desse caso, os legisladores viram-se pressionados a criarem uma lei que tipificasse a conduta de invadir dispositivo informático alheio, com isso surgiu a Lei 12.737, o qual será analisada, passando-se desde a evolução do computador até chegar na sua aplicabilidade, no qual se tecerão comentários acerca das incertezas na interpretação dessa Lei.

Palavras-chave: Transformações. Tecnologia. Dispositivos Tecnológicos. Invasão. Aplicabilidade.

ABSTRACT

The world has gone through several transformations in step with these changes technology has increasingly evolved from there emerged various technological devices, which provided convenience to users, with the provision of various services. However, despite having brought many benefits, some individuals take advantage to commit crimes, computing devices invading and violating privacy. The society is increasingly interacting with computer facilities, and this harvest has increased the number of crimes committed across devices. The case of the actress Carolina Dieckman, who was the victim of an invasion of your computing device, where intimate photographs were obtained, had national repercussions, and, from this case, lawmakers found themselves pressured to create a law that the conduct of tipificasse invading alien computing device, thus arose the Law 12,737, which will be analyzed by passing since the evolution of the computer to get on their applicability, in which it shall comment on the uncertainties in the interpretation of that Act.

Keywords: Transformations. Technology. Technological devices. Invasion. Applicability.

LISTA DE ABREVIATURAS E SIGLAS

Art.	Artigo
Des	Desembargador
ENIAC	Eletronic Numerical Integrator and Calculator
HC	Habeas Corpus
IBM	Internacional Busines Machines Corporation
MS-DOS	Micro Soft Disc Operating System
PC	Personal Cuputer
PLC	Projeto de Lei da Câmara
Rel.	Relator
TI	Tecnologia da Informação
TRF	Tribunal Regional Federal
V	Volume
LAN	Local Area Network

SUMÁRIO

1 INTRODUÇÃO

O presente trabalho pautar-se-á na realização de um estudo acerca dos crimes virtuais, focando-se especialmente na nova forma delituosa que é a invasão de dispositivo informático, bem como a sua aplicabilidade. Este delito, tipificado no art. 154-A do Código Penal, foi uma inovação que a Lei 12.737/2012, vulgarmente chamada de “Lei Carolina Dieckman”, introduziu no referido código.

Com o intuito de atingir o objetivo proposto, seguir-se-ão alguns procedimentos metodológicos a fim de conferir uma maior relevância e cientificidade a presente monografia.

O estudo que será demonstrado apresenta, atualmente, grande relevância em vários meios da sociedade entre os quais está o meio jurídico, pois a criminalidade virtual é uma consequência da globalização desenfreada. A partir desse fato, bem como suas peculiaridades, é que se pautou o interesse na elaboração dessa pesquisa. Acerca desse tema, já existem diversas pesquisas doutrinárias, e com a nova Lei 12.737, passarão a surgir novos posicionamentos, garantindo um maior acevo acerca do desenvolvimento de trabalhos científicos como o presente estudo.

Atualmente, devido a recente entrada em vigor da supracitada Lei, a jurisprudência nacional ainda não apresenta decisões em sede de crimes relacionados à invasão de dispositivo informático. Isso em virtude tanto do pouco tempo da referida Lei, bem como pelas dificuldades que os órgãos de investigação atravessam, muito por causa da precariedade, para combater esses crimes virtuais.

Neste trabalho, segue-se o método dedutivo. Diante disso, com a entrada em vigor da supracitada Lei, serão analisadas e evidenciadas as deficiências dessa legislação no tocante ao tema em foco, enfatizando-se desde a evolução tecnológica até a forma como essa legislação foi criada.

Com relação ao método jurídico será adotado o sistemático, e, nesse sentido, a pesquisa será realizada em uma perspectiva jurídico-penal em vigor no País, que mesmo sendo uma relevante inovação na legislação penal, a Lei encontra-se com problemas e imprecisões. Serão tratados os crimes já existentes anteriores à Lei Carolina Dieckman, praticados a partir de um dispositivo informático.

Os procedimentos técnicos que serão utilizados far-se-ão a partir de uma pesquisa bibliográfica. Assim, na elaboração deste estudo serão consultados materiais que descrevam o assunto, como doutrinas, artigos de internet, pesquisas em sites especializados na matéria e revistas, de forma que vem a justificar essa forma de pesquisa, bem como o embasamento material necessário a presente monografia.

Nesse sentido, primeiramente, serão explanados a progressão histórica acerca da evolução dos dispositivos informáticos, iniciando-se com a criação do computador, passando-se por diversas implementações até chegar aos dispositivos da atualidade, como tablets, smartphones. Também, no primeiro capítulo, serão analisados as redes de computadores e os dispositivos de segurança.

No segundo capítulo será analisada a Lei 12.737/2012, focando-se, principalmente, no art.154-A. Passando-se desde a evolução legislativa, de forma que a lei supracitada foi a primeira a criminalizar a invasão de dispositivo informático, até chegar nas mudanças implementadas nos artigos 266 e 298 do CP.

Por derradeiro, no último capítulo será analisada a aplicação da referida Lei, pautando-se em uma análise dos princípios para uma adequada interpretação, muito por causa das falhas legislativas, bem como os crimes que eram praticados, através de dispositivos informáticos, anteriormente a entrada em vigor dessa Lei.

Assim, o presente trabalho será pautado na inovação legislativa que adveio com a “Lei Carolina Dieckman”, em especial o tipo previsto no art. 154-A, bem como a sua análise, considerando-se as falhas que o legislador cometeu.

2 CONSIDERAÇÕES ACERCA DOS DISPOSITIVOS INFORMÁTICOS

Em linhas gerais, a Lei 12.737 introduziu no ordenamento jurídico penal brasileiro o crime de invasão de dispositivo informático, tipificado no *caput* do art. 154-A, do Código Penal. Para que esse delito seja praticado é necessário que haja a invasão de dispositivo informático alheio, estando conectado ou não a rede de computadores, violando de forma indevida mecanismo de segurança, ou mesmo instala-lo vulnerabilidade para obter vantagem ilícita.

A utilização de dispositivo informático está presente no dia-a-dia de grande parte da população. De forma que, o uso, desses dispositivos, é, sem sombra de dúvidas, um mecanismo da sociedade atual imprescindível para o desenvolvimento das atividades laborativas, bem como no desenvolvimento educacional, na utilização para pesquisa, na comunicação de pessoas distantes entre si a partir das redes sociais, ou mesmo utilizando o dispositivo como instrumento de diversão. Mas, em contrapartida ao desenvolvimento das atividades e de todos os benefícios que são possíveis de realizarem a partir de um dispositivo informático, a todo instante são cometidos inúmeros crimes informáticos muito em virtude de o agente ter a falsa crença de que sua conduta ficará no anonimato, isso devido evolução tecnológica que se tem desenvolvido.

Para garantir uma maior proteção aos dados e informações pessoais contidas nos dispositivos informáticos, foram desenvolvidos meios que possibilitassem uma maior segurança a esses dispositivos. Ainda assim, delinquentes conseguem invadir os dispositivos informáticos, objetivando a obtenção de dados e informações das vítimas, ou instalando vulnerabilidades com fim de obter vantagem indevida.

São vários os dispositivos com a possibilidade de transferências de dados e informações. A partir dessas transferências, interesses surgem e nem sempre com bons propósitos, tornando-se possíveis ameaças à privacidade individual. Mas que dispositivos são esses? Como mantê-los longe das possíveis ameaças? Como são realizadas essas mútuas comunicações? Esses entre outros questionamentos serão explanadas no decorrer deste estudo.

2.1 Da Evolução dos Dispositivos Informáticos

Hodiernamente vivemos um período em que a tecnologia impulsiona cada vez mais o mercado consumerista. A rapidez com que os dispositivos eletrônicos evoluem, faz com que os preços dos produtos, que já estavam em circulação no mercado, diminuam, tornando-se mais acessíveis para os consumidores. E isso, sem dúvidas, é o que está ocorrendo com os computadores, pois, de acordo com a pesquisa realizada e divulgada, em 2011, pela Intel, cerca de 58% dos lares nas regiões metropolitanas do Brasil já possuem computador e cerca de 93% da população que não possuem computador acessa com frequência a internet.

Isso mostra como o computador já faz parte do dia-a-dia da população brasileira, e conforme Gustavo Testa Corrêa (2008, p. 1 e 2):

> Esse fascinante desenvolvimento tecnológico resultou no advento de uma nova era para a humanidade, a denominada ‘Era da Informação’. Pela primeira vez na história, somos capazes de organizar e dominar a informação como nunca, por meio da utilização de computadores, da Internet e de outras tecnologias relacionadas. Sabemos o quanto isso é importante, pois a troca e a difusão de informações, no decorrer do tempo, sempre foram responsáveis pelo desenvolvimento dos mecanismos de transformação social, já que onde houve revoluções houve necessariamente a disseminação de ideais.

Certamente, essa máquina foi uma das maiores invenções já criadas pelo homem e que, a todo instante, passa por aperfeiçoamentos. Mas, em meados do século XIX, antes de ser esta máquina moderna a que dedicamos horas e horas em sua interface, era um computador mecânico, idealizado por Charles Babbage. Este é considerado pela maioria dos cientistas da computação como o verdadeiro pai do computador, levando-se em consideração os modelos que são desenvolvidos atualmente, pois apesar de ter concluído o projeto do primeiro computador, não chegou a desenvolvê-lo, haja vista não existir peças para implementação do seu invento.

Já no final do século XIX, bancado pelos Estados Unidos, Herman Hollerith construiu uma máquina visando diminuir o tempo da análise dos cartões de

recenseamento. Devido ao êxito de suas máquinas, instituiu a empresa *Tabulating Machine Company* que, posteriormente, viria a se chamar de *Internacional Busines Machines Corporation* (IBM), uma das maiores empresas do mundo em Tecnologia da Informação (TI).

A partir da construção do primeiro computador totalmente elétrico, conhecido por ENIAC (Eletronic Numerical Integratorand Calculator), em 1940, passou-se a classificar os computadores em gerações. Três anos antes, Howard H. Aiken e engenheiros da IBM construíram o primeiro computador eletromecânico, o MARK-I, que era automático, depois de iniciado o seu funcionamento não mais necessitava da intervenção humana. Este era mil vezes mais lento que o ENIAC (PIMENTEL, 2000).

Na primeira geração, os computadores, já eletrônicos, funcionavam a partir de válvulas a vácuo. Essa época ficou marcada pela criação da primeira teoria jurídica que teve como objetivo a aplicação do direito às novas tecnologias da época, muito devido aos computadores eletrônicos, haja vista, ter sido formalizado uma nova linguagem jurídica através da lógica simbólica, essa teoria foi batizada por Lee Loevinger com o nome de jurimetrics. Já a segunda geração começou em 1952 e se deu com a comutação das válvulas por transistores, acarretando a redução de tamanho, aumento de desempenho e diminuindo os custos com manutenção.

Em 1964, inícios da terceira geração de computadores, foram criados os circuitos integrados, passou-se a utilizar teclados e monitores, e foi ampliado o incremento dos sistemas operacionais.

Em 1971 surge o microprocessador e, com este, a quarta geração de computadores. Foi também nesta geração que, Bill Gates fundou a Microsoft, e foi criado o sistema operacional MS-DOS (*Micro Soft Disc Operating System*); Steve Jobs e Steve Wozniak criaram a Apple que com o desenvolvimento do segundo computador, o Apple II, propagou o sucesso do computador pessoal (PIMENTEL, 2000).

Atualmente estamos na quinta geração de computadores, que teve início em 1981. As máquinas computacionais da época foram chamadas de computadores inteligentes, isto em virtude do processamento de conhecimentos. Nessa época, com os aprimoramentos das máquinas computacionais, continuou-se reduzindo o tamanho desses dispositivos, pois cada vez mais o hardware, que é a parte física do computador (placa mãe, placa de vídeo, memória, dispositivos de entrada e saída)

tem se tornado menor. Os softwares, que correspondem a parte lógica responsável pela realização dos comandos, foram gradativamente aprimorando-se vindo a possibilitar um relevante aumento no processamento de dados. E assim desenvolveu-se a inteligência artificial.

Foi também nessa época que se difundiu o termo PC (*Personal Cuputer*), através do IBM 5150. Esta terminologia foi amplamente propagada como IBM PC e devido ter obtido um relevante êxito nas vendas, vindo a se consagra mundialmente até os dias atuais. Essa evolução tecnológica não para, pois, a cada dia, os dispositivos informáticos, concomitantemente com a diminuição de tamanho, aumentam o seu desempenho. Tudo isso possibilitou a implementação de novos dispositivos informáticos.

Pensando-se em uma maior praticidade para permitir a utilização em qualquer lugar, foi criado o notebook que se trata, na verdade, de um computador portátil. Hoje em dia, um notebook tem um hardware tão eficaz quanto um computador de mesa, também chamado de desktop, ou popularmente PC (computador pessoal). Mas, assim como ocorreu com este, o notebook não tinha o seu tamanho tão reduzido como é hoje em dia, passando por diversos aprimoramentos, até chegar ao produto que é comercializado atualmente.

O primeiro computador portátil criado foi o Osbone 1, por Adan Osborn. Apesar de ser portátil, pesava em torno de 12 quilogramas e tinha uma tela de 5 polegadas. Com o surgimento e concorrência de novos notebooks, a empresa Osborne faliu. Surge a Compaq, em 1982, com um portátil de melhor desempenho, capaz de compartilhar dados com o IBM PC pessoal.

Ainda em 1982, no Japão, a Epson desenvolve o Epson HX-20 com dimensões de um caderno. Com o crescimento de novos mercados no ramo da informática e a livre concorrência, os notebooks foram aperfeiçoando-se. Em 1985, passam a ser fabricados o TRS-80 model 200 da empresa americana Radio Shack que tinha como atrativo ser o primeiro computador portátil dobrável.

Contudo, foi com o SLT/286, no início da década de 90, que houve um grande avanço tecnológico. O Compaq, ora citado, foi o primeiro notebook a não mais utilizar telas monocromáticas e sim telas VGA (Video Graphics Array) que é um padrão de disposição gráfica para vídeo e foi desenvolvido pela IBM no ano de 1987.

O Thinkpad, fabricado pela IBM, conforme informação disponibilizada por Rodrigo Prada, do portal Tecmundo, foi o primeiro notebook a utilizar o Windows como sistema operacional, isto em 1992. Em 1994, o Thinkpad é submetido a aprimoramentos, passando a ter drive de CD. E, após três anos, esse notebook passa a utilizar drive de DVD. Isto mostra que, com o passar dos anos, a evolução tecnológica fez com que os aparelhos diminuíssem de tamanho e, ao mesmo tempo, não acarretou a diminuição de qualidade, muito pelo contrário, obtiveram um ganho de qualidade inimaginável há 30 anos.

Menores que os notebooks, os netbooks foram lançados, em 2007, pela Taiwanesa Asus. A diferença está desde o tamanho da tela que é menor, no caso do primeiro netbook a tela era de 7 (sete) polegadas, como também o preço que é menor. A configuração é mais básica, sendo utilizado, na maioria das vezes, para acessar a internet. Não possui drive de CD/DVD o que, consequentemente, ajudou na diminuição de tamanho. Por possuir uma tela menor e sua configuração ser inferior ao notebook, o consumo de energia também é reduzido aumentando-se, consideravelmente, a durabilidade da bateria. Por essas entre outras características, sobretudo o preço, o netbook se tornou um sucesso de vendas.

Atualmente o dispositivo tecnológico que está conquistando o gosto do consumidor, e virando a sensação do momento, é o tablet. Apesar desse sucesso vertiginoso, o primeiro conceito a trabalhar uma interface similar aos tablets de hoje em dia, foi no final da década de 80. Naquele momento, conforme informação disponibilizada por Luciano de Sampaio do portal Tecmundo, tais aparelhos eram chamados de *slate computers* ou *pen computrs*.

Até chegar ao que se têm hodiernamente, os tablets passaram por diversos fracassos. Seja por causa da tecnologia aquém ao que temos hoje ou por causa da pouquíssima funcionalidade que tais aparelhos apresentavam, servindo em alguns casos como simples agenda eletrônica de bolso.

O primeiro tablet a ser fabricado, conforme notícia veiculada através do portal Terra, por meio do jornalista Antônio Blanc, foi o GRIDpad da GRID Systems em 1989, já que protótipos como Dynabook de Alan Kay e o Apple Bashful não saíram do papel. Apesar de ser pequeno pra época, haja vista possuir tela de apenas 10 polegadas que era sensível ao toque (*toucscreen*), e possuir modem, conexão com teclado e drive de disquete, o GRIDpad não chegou a ser um sucesso no mercado, pois, em pouco, tempo a empresa faliu.

Já em 2001, a Microsoft lança no mercado uma modificação do Windows XP, chamada de Tablet Edition, que tinha como finalidade fomentar um novo dispositivo informático, o Tablet PC. Devido ao alto custo, ausência de aplicativos e ter que usar uma caneta própria (stylus) para manuseá-lo, o Tablet PC não obteve o resultado esperado.

Mas foi em 2010, com o lançamento do iPad da Apple, que houve uma revolução no mercado informático. Sucesso mundial de vendas, o iPad surgiu devido a empresa Axiotron, a partir de um MacBook da Apple, ter montado um aparelho, o Modbook, com tela sensível ao toque e com sistema operacional MacOS X. Observando o sucesso deste, a Apple desenvolveu e passou a fabricar seu próprio tablet, o iPad, que tornou-se ícone mundial para apreciadores de tecnologia e modelo para desenvolvimento de novos tablets por empresas concorrentes como o Galaxy Tab da Samsung e o Xoom da Motorola.

Concomitantemente ao desenvolvimento dos tablets, um aparelho informático ganhou relevante dimensão mundial, principalmente no mundo corporativo. Conhecido como PDA (Personal Digital Assistent), este aparelho foi desenvolvido com intuito de auxiliar o dia-a-dia, seja na organização de tarefas, na visualização de email, ou no gerenciamento de contatos. Logo, como próprio nome já diz, é um verdadeiro assistente pessoal digital.

Com dimensões que facilitavam o seu deslocamento, já que cabia na palma da mão, com tela sensível ao toque, e algumas funcionalidades voltadas para execução de tarefas, este portátil logo se tornou um aparelho dimensionado ao trabalho. Contudo, por não realizar ligações e com a crescente evolução dos celulares, hoje em dia, estes aparelhos perderam espaço para os smartphones.

Com um smartphone, além de efetuar e receber ligações pode, através de seus aplicativos, executar diversas funções tais como tirar fotografias e posta-las em redes sociais, proceder a localização correta em uma cidade, quando aparelho possuir GPS que é um sistema de posicionamento global via satélite, ou até mesmo pagar boletos bancários utilizando a internet.

Smartphone traduzindo para o vernáculo significa telefone inteligente. É considerado uma junção de PDA, por ser este considerado um extensão de um computador, com um telefone, haja vista ser ainda, uma de suas funções, a realização de ligações.

Outros dispositivos, como os *pendrive* e HD (*Hard Disk*) ou disco rígido, são utilizados especificamente para armazenamento e transferência de dados. Devido a portabilidade e grande capacidade de armazenamento auxiliam no dia-a-dia.

Todos esses aparelhos vistos anteriormente evoluíram, praticamente, ao mesmo tempo. De forma que, com a evolução tecnológica e uma sociedade cada vez mais consumerista, as inovações ocorreram em pequenos intervalos de tempo.

Com o transcorrer do tempo, os dispositivos informáticos foram se integrando, passando a compartilhar dados e informações. Todos possuem conectividade via USB, alguns dispositivos, os mais antigos, utilizam infravermelho, os mais novos Bluetooth, e outros se conectam através de rede WiFi que é uma comunicação sem fio e pode ser utilizada para acessar internet ou mesmo para integrar diversos dispositivos como um notebook a um tablet. Assim, da mesma forma que facilita a transferência de informações de um dispositivo para outro, também pode ser utilizada para obtenção indevida dessas informações.

Logo, com a disseminação desses dispositivos informáticos, cada vez mais é possível testemunhar o número elevado de casos de invasão de tais aparelhos. E uma das formas que os criminosos utilizam para possibilitar essa invasão, acreditando ficar impunes e invisíveis para uma possível investigação, é a internet.

2.2 Conceito e Espécies de Rede de Computadores

Rede de computadores consiste em 2 ou mais computadores se interligarem entre si, possibilitando o compartilhamento de recursos físicos e lógicos, podendo ser dados, impressoras, e-mails, entre outros.

Atualmente os dispositivos informáticos, em sua grande maioria, podem conectar-se entre si, facilitando a transferência de dados. É, sem duvidas, a internet, o grande facilitador dessa troca mútua de informações. Esta é apenas uma das possíveis redes de computadores, mas, devido a sua dimensão global, é a que mais se sobressai.

Também são consideradas como redes de computadores, uma rede local ou uma rede de telefonia. Esta, apesar de ser a de maior abrangência, não é a mais

utilizada, sendo a internet, em face de sua relevância e crescente expansão, o principal veículo de transferência de dados e informações.

2.2.1 Internet

Conforme as palavras de Eric Schmidt, trazido por Gustavo Corrêa (2008, p. 7) “A Internet é a primeira coisa que a humanidade criou e não entende, a maior experiência de anarquia que jamais tivemos”. Além de sua complexidade é um sistema grandioso, haja vista uma pessoa poder interagir com o mundo sem sair de casa.

Considerada um mundo em suas mãos, a Internet nos ensinamentos de Gustavo Corrêa (2008, p. 8):

> [...] É um sistema global de rede de computadores que possibilita a comunicação e a transferência de arquivos de uma máquina a qualquer outra máquina conectada na rede, possibilitando, assim, um intercâmbio de informações sem precedentes na história, de maneira rápida, eficiente e sem a limitação de fronteiras, culminando na criação de novos mecanismos de relacionamento.

A internet começou a galgar seus passos, e transformar no que temos hoje, na década de 60. Primeiramente sua finalidade era essencialmente militar, já que foram os americanos que a desenvolveram com a finalidade de se defender ao se comunicarem entre instituições, e ao mesmo tempo ser uma arma na guerra fria (CORRÊA, 2008).

A sociedade passou a utiliza-la, como bem anota Alexandre Pimentel (2000, p. 45), “Com o fim da Guerra Fria, a ***rede***, que mais tarde veio a receber o nome de **Internet**, teve seu acesso a partir de então disponibilizado para o público em geral”.

O crescente número de usuários é devido às facilidades que a internet traz consigo, seja para ficar atualizado no que acontece no mundo, para pesquisar e obter informações acerca de determinado conteúdo, ou para realizar compras ou fazer transferências bancárias sem sair de casa, ou mesmo para entretenimento nas diversas redes sociais.

Assim, em razão da infinidade de tarefas que a rede possibilita, tem aumentado o número de pessoas integradas a essa rede, de forma que mais de 200 (duzentas) milhões de pessoas, em 2008, espalhadas por todo o mundo, eram usuárias da internet (CORRÊA, 2008, p. 9), e em 2011, segundo a União Internacional de Telecomunicações (UIT), alcançou o expressivo número de dois bilhões de usuários dessa fascinante rede de computadores.

Logo, da mesma forma que cresce o número de usuários na grande rede de computadores também é crescente o número de vítimas desse sistema, haja vista muitos se aproveitarem para cometerem ilícitos, pois, "[...] Qualquer indivíduo que tenha acesso à Internet, desde que possua alguns conhecimentos de informática, pode invadir banco de dados existente no mundo inteiro [...]" (CRUZ, 2006, p. 12).

Nos termos de Gustavo Testa Corrêa (2008, p. 44):

> A Internet é um paraíso de informações, e, pelo fato de estas serem riqueza, inevitavelmente atraem o crime. Onde há riqueza há crime. Constatamos a fragilidade dessa riqueza quando percebemos que sinais digitais, representando vastas quantias de dinheiro, podem ser interceptados e "furtados". Em vez de pistolas automáticas e metralhadoras, os ladrões de banco podem agora usar uma rede de computadores e sofisticados programas para cometerem crimes [...].

Como foi visto, alguns utilizam a Internet para o cometimento de crimes. Além dessa também existem outras redes que podem ser utilizadas para práticas de delitos, como as redes locais.

2.2.2 Rede de área local (LAN)

Rede de área local ou mesmo rede local é uma rede utilizada em uma pequena dimensão geográfica, geralmente em locais fechados, como empresas, escolas, universidades. Conforme Evandro Cantu (2003, p. 64) "Numa rede local, todos os computadores e demais dispositivos de rede são diretamente conectados [...]". Assim, estabelecem conexões individuais entre os computadores e dispositivos.

Dentre outras redes a Ethernet, que não se confunde com Internet, é a mais utilizada. Nas palavras de Cantu (2003, p.65) “Ethernet é a tecnologia de redes mais difundida atualmente. Pode-se dizer que a Ethernet está para as redes locais, assim como a Internet está para as redes geograficamente distribuídas de alcance global”.

Assim, em ambientes pequenos que necessitam da troca mútua de dados e informações são utilizados redes locais, pois quanto maior for a distância mais dificultoso fica a transferência de informações. Apesar de ter uma dimensão menor, essas redes também são passíveis de invasões e certamente no cometimento de delitos.

2.3 Mecanismo de Segurança e Vulnerabilidade

Falar em segurança é rotineiro e recorrente, haja vista as notícias diárias que trazem, geralmente, como matéria principal, a violação de direitos, aumento da criminalidade, em consequência da falta de segurança. Segurança que deveria ser garantida pelo governo, pois está consagrado no art. 144, da Constituição Federal como sendo um dever do Estado.

Diferentemente dessa segurança que é dever do Estado, a segurança digital, ou da informação, tem caráter privado e objetiva resguardar informações de interesse particular. Nessa seara, a demanda por segurança informática tem crescido vertiginosamente, muito devido as diversas preocupações sobre o uso, sem a devida autorização, de dados e informações privadas e possíveis consequências.

Assim, ter segurança é a forma de proteger dados, informações e sistemas contra erros atuações maliciosas de agentes, sem a devida autorização a fim de diminuir a probabilidade de incidentes de segurança.

Existem várias formas de manter os dispositivos seguros. Entre outras, a senha é uma das formas de restringir o acesso indevido de tais aparelhos, bem como a utilização de *antimalware* e *firewall*.

A senha é uma forma de limitar a utilização de um aparelho, fazendo com que somente os conhecedores daquela tenham acesso ao dispositivo. Desde os computadores pessoais ou até mesmo alguns pendrives e HD externos podem

utilizar da senha como limitador de acesso. Sendo considerada forma de autenticação mais utilizada.

O *antimalware* é um programa utilizado para combater os *malware* ou códigos maliciosos. Ou seja, são programas utilizados para combater outros programas ou infecções. Esse geralmente tem o propósito de obter dados e informações de forma indevida.

Já o *firewall* é um dispositivo de segurança que tem a função de interceptar as transferências de informações sem a devida autorização. Assim, dificulta a atuação de pessoas má intencionadas na obtenção de determinado conteúdo.

Essas são algumas formas de manter os dispositivos seguros impedindo a atuação de um *hacker*. Este, que nas palavras de Gustavo Testa Corrêa (2008, p. 59) “[...] é um indivíduo que tem a intenção, através do computador, de adentrar um sistema sem autorização”. Assim, para manter os dispositivos seguros, a utilização de tais mecanismos é de extrema relevância.

3 ANÁLISE DAS INOVAÇÕES INTRODUZIDAS PELA LEI 12.737/2012 NO ORDENAMENTO PENAL BRASILEIRO.

Como foi visto supra, a tecnologia referente à informática tem evoluído rapidamente, principalmente nas últimas décadas, haja vista o elevado número de aparelhos digitais que surgem e que auxiliam cada vez mais nas atividades laborais, ou mesmo para o entretenimento. O computador, sem sobra de dúvidas o maior símbolo dessa nova era, passou por diversos aprimoramentos até se tornar um aparelho indispensável na atualidade. Surgiram novos equipamentos como o notebook, o celular, o PDA, e mais recentemente, o smartphone e o tablet.

Diante de tamanha evolução tecnológica, diversos indivíduos, aproveitando-se desta, aplicam seus conhecimentos informáticos em desacordo com a moral, a honestidade, os princípios éticos. Utilizam-se da tecnologia como meio, por ser esta uma forma dificultosa de identificação dos agentes e suas condutas, facilitando o anonimato e auxiliando no cometimento de crimes contra a honra, fraudes, violação de direito autoral, entre outros.

3.1 Breve Abordagem Acerca Da Origem Da Lei 12.737/2012.

No ano de 2012, devido à divulgação e repercussão na mídia de algumas fotografias íntimas da atriz Carolina Dieckmann, foi que o legislador infraconstitucional apresentou uma proposta de lei, na perspectiva de combater e punir as invasões de dispositivos informáticos. Foi a partir dessa proposta de lei, a PLC (Projeto de Lei da Câmara) 35/2012, de autoria do deputado Paulo Teixeira, que deu origem à Lei 12.737.

Anteriormente a essa, somente aquelas condutas já tipificadas como crime poderiam ser punidas, pois conforme o princípio da legalidade (da reserva legal) insculpido no art. 1º, do Código Penal, “Não há crime sem lei anterior que o defina, não há pena sem prévia cominação legal” e também consagrado no art. 5º, XXXIX da Constituição da República Federativa do Brasil.

Acerca disso, Uadi Lammêgo Bulos (2007, p. 254) leciona:

> A Constituição de 1988 compactua-se com o art. 1º do Código Penal: "Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal", semelhante ao velho aforismo latino *Nulla crimen nulla poena sine praevia lege*. Prestou homenagem à *tipicidade penal*. Típico é o fato que subsume ao comportamento delituoso, prescrito nas normas penais incriminadoras pelo legislador infraconstitucional.

Ao longo dos anos, o legislador pecou por sua omissão em não legislar sobre a criminalidade informática. E só o fez devido ao clamor midiático do caso, supracitado, da atriz Carolina Dieckman, que inclusive nomeia informalmente a Lei 12.737/2012. A partir desse caso também foi criado a Lei 12.735, conhecida por "Lei Azeredo", originado pelo projeto 85/1999, logo, desde o final da década de 90 que essa lei tramitava no Congresso e não era devidamente votada.

Não foi a primeira vez e nem será a última que o legislador infraconstitucional somente fará jus ao que de si é esperado, que é a atividade legiferante, a partir de uma motivação da mídia ou mesmo da sociedade. Tal ocorreu, de igual forma, no enquadramento do homicídio qualificado como crime hediondo. Monteiro apud Gomes (2012), ao tratar do referido enquadramento, assim explica:

> Atende, sobretudo, a anseios populares, já que o projeto de lei que deu origem à Lei n. 8.930, de 06 de setembro de 1994, foi incentivado por mais de um milhão de assinaturas, campanha liderada pela escritora Glória Perez, mãe da atriz Daniella Perez, assassinada de forma brutal no dia 28 de dezembro de 1992, e por Jocélia Brandão, mãe da menina Míriam, sequestrada e morta por dois rapazes em Belo Horizonte, no início de 1993.

Isso mostra que a atividade legislativa em certas ocasiões é impulsionada a partir de situações ocorridas e repercutidas fora do parlamento, influenciando de forma direta na produção das leis que nem sempre têm a precisão que delas se esperam. É o caso da Lei 12.737/2012 que, mesmo sendo uma relevante inovação legislativa, vem sendo criticada devido à ausência de esclarecimento a certos termos técnicos, o que poderá ocasionar em algumas distorções na aplicação dessa lei.

Diferentemente de nossos representantes, o Congresso americano já legislava sobre o tema desde 1970 que nas palavras de Pâmela Moura (2012) “[...] estão entre os pioneiros na questão da legislação aplicável aos cibercrimes”. Nesse sentido, aduz Rosa apud Moura (2012, p. 30):

> Os EUA começaram a legislar sobre os crimes de informática no fim da década de 1970; a primeira lei federal sobre crimes de informática foi a Computer Fraud anda Abuse Act – CFAA, de 1986, que criminalizava condutas como, por exemplo, o acesso não autorizado, seja para obtenção de segredos nacionais com intenção de prejudicar os EUA, seja para obter informações financeiras e de créditos, ou, ainda, o simples acesso não autorizado a computador do Governo Federal.

É bem verdade que os americanos destacam-se mundialmente no desenvolvimento informático, mas são mais de quarenta anos de atraso legislativo do Brasil em relação a eles. E outros países como a Inglaterra em 1990 e Portugal em 1991 tipificaram condutas para reprimir delinquentes cibernéticos (Moura, 2012).

3.2 Análise dos Elementos Específicos do Crime de Violação de Dispositivo Informático, Descrito No Art. 154-A Do Código Penal Brasileiro.

A redação do art. 154-A do Código Penal assim dispõe:

> Art. 154. Invadir dispositivo informático alheio, conectado ou não a rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem a autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidade para obter vantagem ilícita.

Essa conduta, que tipifica a violação de dispositivo informático, está inserida no Título I (Crimes Contra a Pessoa), Capítulo VI (Crimes Contra a Liberdade Individual), Seção IV (Crimes Contra a Inviolabilidade dos Segredos) na Parte Especial do Código Penal de 1940.

Buscando proteger os dados e informações contidos em dispositivos informáticos, o legislador enquadrou a conduta no capítulo de Crimes Contra a Liberdade Individual. Esta liberdade, que está ligada à intimidade das pessoas e é constantemente devassada por delinquentes ao violarem dispositivo informático, está consagrada na Constituição da República Federativa do Brasil como um direito fundamental, conforme o art. 5º, caput:

> Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e a propriedade, nos seguintes termos. [...] X – São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

Nas palavras de José Afonso da Silva (2008, p. 209 e 210):

> [...] O amplo sistema de informações computadorizadas gera um processo de esquadrinhamento das pessoas, que ficam com sua individualidade inteiramente devassada. O perigo é tão maior quanto mais a utilização da informática facilita a interconexão de fichários com a possibilidade de formar grandes bancos de dados que desvendem a vida dos indivíduos, sem sua autorização e até sem seu conhecimento.

Assim, através da conduta tipificada pelo legislador penal objetiva-se resguardar o direito à intimidade bem como ao segredo, este, considerando a acepção da palavra e enquadrando-o dentro do tipo, é considerado propriamente o sigilo dos dados informáticos.

3.2.1 Definição do sujeito ativo e do sujeito passivo.

Quanto ao sujeito ativo, o crime definido no art. 154-A é considerado comum, pode ser praticado por qualquer pessoa. Apesar de não ser necessária

qualquer qualidade especial, mesmo que o funcionário público venha a praticar o crime não haverá nenhum aumento de sua pena.

Já o sujeito passivo é aquele que é dono, possuidor, ou mesmo quando está utilizando dispositivo informático de um amigo. Assim entende Bittencourt (2012) que "[...] será igualmente o titular do conteúdo constante do dispositivo violado ou invadido, mesmo que se trate de pessoa diversa". Também comunga desse mesmo pensamento, Cabette (2013), ao obtemperar que:

> O sujeito passivo da infração é, portanto, qualquer pessoa passível de sofrer dano moral ou material decorrente da ilícita obtenção, adulteração ou destruição de dados ou informações devido à invasão ou violação de seu sistema informático, mediante vulneração de mecanismo de segurança. Assim também é sujeito passivo aquele que sofre a instalação indevida de vulnerabilidades em seu sistema para o fim de obtenção de vantagens ilícitas. Na verdade, qualquer pessoa que tenha sua privacidade violada pelo invasor é sujeito passivo da infração. Por exemplo: um amigo usa o computador de outro para conversas particulares via internet, cujo conteúdo é ali armazenado por meio de senha. Alguém invade o sistema informático daquele computador e viola a privacidade, não do dono do computador, mas do seu amigo. Ora, este segundo também é vítima do crime. [...]

Assim, também poderá ser sujeito passivo não só as pessoas físicas, mas também as pessoas jurídicas de direito público, como a administração pública direta e indireta da União, Estados, Distrito Federal e Municípios, bem como as pessoas jurídicas de direito privado, como empresas privadas.

Conforme o § 5º, do art. 154-A do Código Penal, caso o sujeito passivo seja o Presidente da República, um governador, um prefeito, o Presidente do Supremo Tribunal Federal, o Presidente da Câmara dos Deputados, do Senado, de Assembleias estaduais, da Câmara do Distrito Federal ou de câmaras municipais; ou ainda dirigente máximo da administração direta e indireta, seja federal, estadual, municipal ou do Distrito Federal, haverá um aumento na pena do delinquente de um terço à metade.

3.2.2 Condutas e elementares normativas.

Conforme já visto anteriormente o bem jurídico tutelado pela tipificação penal constante no art. 154-A do Código Penal é o sigilo na utilização do dispositivo informático e, secundariamente, a intimidade e a vida privada.

Os verbos presentes nesse tipo penal são dois, tratando-se, é bem verdade, de um crime de ação múltipla. Assim, o delinquente praticará um único crime mesmo realizando os dois núcleos do tipo. O primeiro verbo, invadir, inicia o próprio tipo, tendo o significado de “violar ou ingressar, clandestinamente, isto é, sem autorização ou permissão de quem de direito, sem o consentimento do proprietário ou titular do *dispositivo informático*.” (Bittencourt, 2012).

Nas palavras de David Pimentel Barbosa de Siena (2013):

> [...] O verbo invadir, eleito como figura nuclear, possui significação semântica de “entrar à força ou sem direito”. Obviamente que os modos de execução da conduta típica normalmente são incompatíveis com a presença da violência ou grave ameaça à pessoa, pois se fizerem presentes será o caso de imputação de crime mais grave. Assim sendo, o verbo em questão deve ser entendido como “entrar sem direito ou sem autorização”.

Logo, caso o agente pratique a conduta de invadir empregando violência ou grave ameaça, poderá incorrer em um crime mais grave. Também se faz necessário que o agente efetue a invasão contra dispositivo informático alheio. Este elemento normativo remete a ideia de que o dispositivo deverá ser de outra pessoa, pois, não existiria invasão se fosse contra o próprio dispositivo.

A conduta poderá ser praticada através da rede mundial de computadores ou fora dela. Assim, aduz o Bittencourt (2012):

> [...] É irrelevante que o dispositivo violado encontre-se conectado a rede mundial de computadores, conhecida como internet. Em outros termos, a proteção penal não é da rede mundial de computadores, mas da privacidade individual, pessoal ou profissional do indivíduo.

Assim, estarão sob a guarida do artigo supracitado tanto os dispositivos conectados à internet, bem como aqueles que mesmo não estando conectados, possam armazenar dados e informações, como celular, pen drive, HD externo entre outros. Contudo, somente estarão tutelados aqueles dispositivos que possuírem mecanismo de segurança, que nas palavras de Siena (2013) "[...] barreiras físicas ou virtuais que impedem ou limitam o acesso à informação por parte de terceiros mal intencionados". Diante disso, aqueles que não possuírem tal mecanismo, ou, este não estiver em pleno funcionamento, não configurará a conduta descrita no tipo, haja vista a invasão do aparelho informático estar diretamente vinculada à violação indevida de dispositivo de segurança, onde o elemento normativo "indevida" remete a ideia de ausência de autorização.

Em seu trabalho, Cabette (2013) pondera que "o acesso a informações disponibilizadas livremente na internet e redes sociais (v.g. Facebook, Orkut etc.), sem qualquer barreira de privacidade não constitui qualquer ilegalidade". Logo, aquele que disponibiliza imagens na internet com acesso livre não estará protegido pelo dispositivo penal ora em comento.

O agente deverá realizar pelo menos uma das finalidades contidas no tipo. Ou seja, deverá obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo, de outra forma não outra solução senão a atipicidade da conduta.

Assim, pondera Bittencourt (2012), ao lecionar que:

> [...] A conduta incriminada, no caput, de "invadir" dispositivo informático alheio deve ser, necessariamente, praticada "com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo" violado. A ausência dessa finalidade especial afasta a adequação típica. Se a finalidade dessa conduta for outra, se crime existir, certamente, não será este.

Logo, caso não ocorram essas finalidades específicas, a conduta praticada pelo agente será considera atípica, podendo o mesmo responder por outro crime, mas não o de violação de dispositivo informático.

O crime em análise, como já foi visto anteriormente, trata-se de um tipo penal misto alternativo. De forma que, "instalar", é o núcleo da segunda conduta descrita no tipo. Na prática dessa conduta, o delinquente instala, no dispositivo

informático, vulnerabilidade com a finalidade de obter vantagem ilícita. Assim pontifica Siena (2013):

> O segundo especial fim de agir, previsto alternativamente pelo legislador penal, corresponde a instalar (processo destinado a colocar todos os dados necessários em um hardware para que determinado software possa ser executado) vulnerabilidades (abertura ou brecha em um sistema operacional, normalmente indesejada e oculta, que pode ser utilizada pelo invasor para executar códigos maliciosos) para obter vantagem ilícita (patrimonial ou extrapatrimonial).

Nessa mesma linha segue Sanches (2013, p. 263) ao ponderar que:

> [...] O cibercriminoso instala no dispositivo vulnerabilidades, isto é, brechas no sistema computacional (conhecidos como “bugs” ou “worms”) para espalhar software malicioso que serve para atacar, degradar, impedir a utilização correta de um equipamento ou obter informações de forma encoberta, visando o agente conquistar vantagem ilícita.

Um exemplo desse da instalação de vulnerabilidade ocorre quando um indivíduo invade um dispositivo informático e nele instala algum tipo de programa que tenha como função a revelação de senhas digitadas pelo usuário do dispositivo.

3.2.3 Forma equiparada.

O § 1º, do art. 154-A do Código Penal, equipara a conduta descrita nesse parágrafo com a conduta descrita no caput do artigo supra. Logo existe uma vinculação da primeira com a segunda. Este parágrafo descreve as condutas de produzir, oferecer, distribuir, vender ou difundir dispositivo ou programa de computador com a intenção de que seja praticada a invasão de dispositivo informático alheio. Assim, trata-se de crime de ação múltipla, o que implica dizer que mesmo que delinquente pratique mais de uma dessas condutas, praticará apenas um único crime.

Com o brilho que lhe é peculiar, Greco (2013), diz que:

> *Produzir* significa criar, gerar, fabricar; *oferecer* importa em ofertar, gratuita ou onerosamente; *distribuir* tem o sentido de partilhar, repartir; *vender* tem o significado de transferir (o dispositivo ou o programa de computador) mediante um preço determinado; *difundir* diz respeito a propagar, divulgar, espalhar. [...] as condutas acima narradas devem ser cometidas *com o intuito de permitir a prática da conduta definida no* caput do citado dispositivo legal, ou seja, o agente produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador, no sentido de permitir com que terceira pessoa invada 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 (grifo do autor).

O agente não atua diretamente na conduta descrita no caput, mas sim como cúmplice, pois colabora com que terceiro invada o dispositivo informático. Assim, o objetivo do legislador, com relação à participação criminosa, foi buscar a incriminação das suas formas mais comuns.

3.2.4 Formas qualificadas.

O legislador criou, no parágrafo 3º do art. 154-A, uma forma qualificada do delito, tornando o crime mais grave a partir de uma nova circunstância, elevando-se a pena, que no tipo básico é de 03 (três) meses a 01 (um) ano, e multa, para 06 (seis) meses a 02 (dois) anos. Ambas as condutas são consideradas crimes de menor potencial ofensivo, nos termos a Lei 9.099/95.

Diz o referido parágrafo que o crime qualifica-se a partir da invasão, caso resulte na obtenção de dados de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações secretas, assim definidas em lei, ou o controle remoto do dispositivo invadido, desde que não autorizado.

Sobre a primeira parte da qualificadora subscrita no § 3º, Maggio (2012) elucida que:

> São três hipóteses: (1) obtenção de conteúdo (ou simples conhecimento do teor) de comunicações eletrônicas, como, por exemplo: do Correio Eletrônico (*e-mail*) e do SMS (*Short Messaging Service*), por meio dos quais é possível enviar e receber mensagens de texto, imagens, vídeos e clipes de áudio etc.; (2) obtenção de segredos comerciais ou industriais (exemplos: fórmulas, desenhos industriais e estratégias para lançamento de produtos); (3) obtenção de informações sigilosas, assim definidas em lei (norma penal em branco). Tratando-se de violação de sigilo bancário ou de instituição financeira (Lei 7.492/86, art. 18), o crime é mais grave (reclusão, de um a quatro anos, e multa) e, assim, o agente responde por esse e não pelo delito de invasão de dispositivo informático qualificado em estudo.

Assim, caso ocorra conflito entre as normas, será utilizada o princípio da especialidade para sanar o conflito, prevalecendo a conduta que for tipificada em crime mais grave, mesmo porque o tipo qualificado é uma norma penal em branco merecendo, ainda, complementação, para que se obtenha uma adequada interpretação.

Já na segunda parte do tipo qualificado o legislador procurou enquadrar como criminosos aqueles que manipulam um dispositivo, longe deste, a partir de outro dispositivo utilizando-se de programas capazes de tal sortilégio.

Com maestria, Sanches (2013, p. 265) nos esclarece que:

> [...] O dispositivo informático do agente passa a se denominar guest (hóspede), e o da vítima *host* (hospedeiro). Essa figura qualificada ocorre quando, após a invasão, o agente instala um programa para acesso e controle remoto do dispositivo, sem a autorização da vítima.

Logo, nessa conduta, o dispositivo da vítima fica submisso à manipulação do criminoso, que terá livre acesso e poderá comandar todos os dados e informações presentes no dispositivo informático.

3.2.5 Causas de aumento de pena.

Haverá majoração, conforme § 2º do art. 154-A, quando, a partir da invasão, resulte prejuízo econômico, material ou financeiro, para a vítima. A pena será aumentada de um sexto a um terço. No caso do parágrafo supracitado, a majoração

incidirá sobre as condutas tipificadas no caput e as do § 1º. Assim posiciona-se Sanches (2013), elucidando que “pela posição topográfica da majorantes percebe-se que § 2º incide nas figuras previstas no *caput* e § 1º; já o aumento do § 4º recai sobre a forma qualificada do delito”.

Já a majorante do § 4º, incidirá sobre a figura qualificada do § 3º, de forma que será aumentada a pena de um a dois terços, em caso de divulgação (dar notoriedade), comercialização (atividade relacionada ao negócio, compra e venda) ou transmissão a terceiro, a qualquer título dos dados ou informações obtidos.

3.2.6 Elemento subjetivo.

O elemento subjetivo no delito de invasão de dispositivo informático é o dolo, que é caracterizado pela consciente e livre vontade de violar dispositivo alheio, a partir da violação indevida de mecanismo de segurança ou instalando vulnerabilidade no aparelho. Assim é o posicionamento de Sanches (2013, p. 264) ao transcrever que:

> O tipo prevê elementos subjetivos específicos, representados pelas expressões “com o fim de obter, adulterar ou destruir dados ou informações” e “para obter vantagem ilícita”. Logo, ausentes essas finalidades especiais, o fato passa a ser um indiferente penal.

Diante disso, não existe previsão quanto ao cometimento da conduta descrita no tipo, a título de culpa. Já no § 1º, o agente deve ter a intenção de permitir que a seja praticada a conduta descrita no caput.

3.2.7 Consumação e Tentativa.

O crime estará consumado quando o agente invadir o dispositivo informático alheio, violando indevidamente mecanismo de segurança, sabendo-se que age sem

a necessária permissão. Não depende, para a consumação do delito, de concretização do dano, mas tão somente torná-lo possível. Assim obtempera Sanches (2013, p. 264):

> Trata-se de um crime formal (ou de consumação antecipada), perfazendo-se no momento em que o agente invade o dispositivo informático da vítima, mediante violação indevida de mecanismo de segurança, ou nele instala vulnerabilidades, independentemente da produção do resultado visado pelo invasor.

É considerado um crime plurissubsistente, pois não se trata de crime de ato único, admitindo-se, assim, tentativa, mesmo sendo difícil a sua constatação.

3.2.8 Ação Penal.

A Lei 12.737/2012 também introduziu no Código Penal o art. 154-B. Este dispositivo traz em seu texto o manejo da ação penal. De forma que, em regra, por tratar-se de um bem jurídico disponível, a ação penal é pública condicionada à representação. É possível que o ofendido venha a consentir, nesse caso, não restará outra solução senão a exclusão da adequação típica.

Contudo, o bem jurídico poderá deixar de ser disponível, caso o crime seja cometido contra a Administração Pública direta e indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos. Nesse caso, a ação será pública condicionada à representação.

4 APLICAÇÃO DA LEI 12.737

Para que lei atinja o fim a que se propôs, desejado pelo legislador com a sua feitura, deve interpreta-la buscando de forma precisa transpassar a sua real finalidade.

Assim, para aplicar a lei deve realizar a interpretação, que:

> [...] Consiste em extrair o significado e extensão em relação a realidade. É uma operação lógico-jurídica que se dirige a descobrir a vontade da lei, em função de todo o ordenamento jurídico e das normas superiores de cultura, a fim de aplica-las aos casos concretos da vida real (JESUS, 2010).

De forma harmônica ao analisar a lei, os princípios são instrumentos de extrema eficácia na aplicação da lei.

Seguindo essa linha Nucci (2012, p.47) pondera que:

> [...] No sentido jurídico, não se poderia fugir de tais noções, de modo que o conceito de princípio indica uma ordenação, que se irradia e imanta os sistemas de normas, servindo de base para a interpretação, integração, conhecimento e aplicação do direito positivo.

Logo, os princípios são basilares para uma interpretação adequada, pautando-se em garantir a liberdade bem como a segurança dos indivíduos, e também a própria norma penal.

4.1 Princípios Concernentes a Aplicação da Lei 12.737

Os princípios servem de fundamento para os diversos ramos do direito, o Direito Penal não é diferente. Exercem um papel de sustentáculo e ao mesmo tempo equilíbrio e ponderação para a evolução da norma, isso em virtude da constante mudança que atravessa a sociedade. Luiz Regis Prado (2012, p. 156) pondera que

“o Direito Penal do futuro deve orientar-se no sentido da mantença dos princípios garantistas não só para o sistema e o Estado de Direito, mas sobretudo para os indivíduos”.

É bem verdade que o princípios são garantias, que estão consagradas na Constituição Federal, bem como limitadores ao poder punitivo e opressor exercido pelo Estado.

Seguindo esse entendimento Paulo Queiroz (2012, p. 48), pondera que:

> A Constituição Federal (1988), apesar de seu caráter generalíssimo, constitui a legislação jurídico-penal fundamental, porque define princípios e garantias penais e processuais penais, estabelece limites à intervenção penal e prevê mandados de criminalização e não criminalização, de penalização e não penalização (art. 5º).

Como bem se sabe, a Constituição é hierarquicamente superior às demais legislações, seja a partir de garantias, ou mesmo limitando o poder punitivo (*jus puniende*) exercido pelo Estado, e até mesmo limitando o direito penal.

4.1.1 Princípio da legalidade

Anteriormente já tratado, a Lei 12.737, que foi uma inovação na seara penal há muito desejada, prolongou-se por muitos anos até a sua feitura. E como se sabe, sem lei não há crime e não há punição ao agente causador do fato.

Assim, respeitando-se o princípio da legalidade, que nas palavras de Rogério Sanches (2013, p. 76), “trata-se de real limitação ao poder estatal de interferir na esfera de liberdades individuais**,** [...]” só haverá punição aos delinquentes, aquelas condutas praticadas a partir do dia 2 de abril de 2013, nessa data passou a vigorar os tipos incriminadores da Lei 12.737 de 2012.

Nessa mesma linha de pensamento, Julio Mirabete e Renato Fabbrini (2010, p. 39) afirmam:

> [...] Ainda que o fato seja imoral, antissocial ou danoso, não haverá possibilidade de se punir o autor, sendo irrelevante a circunstância de entrar em vigor, posteriormente, uma lei que o preveja como crime.

O principio da legalidade ou da reserva legal conforme pondera Luiz Regis Prado (2012, p. 158), ao mesmo tempo em que traz o ensinamento de Navarro Frias:

> Atualmente, seu fundamento radica na proteção dos valores segurança jurídica, liberdade e igualdade, por meio da vinculação dos Poderes Públicos à lei precisa e concreta, “o que garante que seja o legislador quem adote as decisões básicas na matéria, exclui a arbitrariedade no exercício do poder punitivo do Estado e assegura o tratamento igualitário na lei e na aplicação da lei”.

Assim, tal princípio tem o condão de coibir abusos realizados pelo Estado, propiciando a segurança jurídica necessária, até porque, o Direito Penal lida com direito à liberdade e, ao mesmo tempo, tem a função de proteger bens jurídicos indispensáveis para o bom convívio dos homens em sociedade.

Em sua obra, Rogério Greco (2010, p. 91) pontifica que:

> Por intermédio da lei existe a segurança jurídica do cidadão de não ser punido se não houver uma previsão legal criando o tipo incriminador, ou seja, definindo as condutas proibidas (comissivas ou omissivas), sob a ameaça de sanção.

Mas, para que haja aplicação ao caso concreto, ponderando entre o direito a liberdade, consagrado pela Constituição Federal, no art. 5º, LIV, “ninguém será privado da liberdade ou de seu bens sem o devido processo legal”, e o poder punitivo do Estado, é preciso que a lei já esteja em vigor. Ou seja, caso não haja conciliação entre a data de publicação e a data estabelecida para sua vigência, ocorrerá a *vacatio legis*, ou período entre a publicação e a vigência.

Diante disso, Greco (2010, p. 97) também leciona que:

> [...] A lei penal que contenha tipos penais incriminadores ou que de qualquer forma agrave a situação do agente, aumentando, por exemplo, hipóteses de circunstâncias agravantes, criando causas de aumento de pena etc., só pode ser aplicada, ou mesmo obedecida, após a sua entrada em vigor.

Tratando-se dessa Lei, o legislador comtemplou um bem jurídico de extrema relevância ao tutelar a privacidade individual, esta, "[...] confere ao indivíduo a possibilidade de conduzir sua própria vida da maneira que julgar mais conveniente, sem intromissão da curiosidade alheia" (NOVELINO, 2012, p. 503 e 504), configurada a partir do armazenamento de dados e informações contidas em um dispositivo informático.

Logo, para que a conduta praticada pelo agente seja enquadrada como crime de invasão de dispositivo informático, deverá tê-la sido praticada posterior a entrada em vigor da lei. Pois mesmo que já tenha sido publicada, a lei não poderá ser utilizada na incriminação do delinquente.

Assim, somente condutas que, mesmo praticadas a partir da invasão de dispositivo informático, já eram previstas na legislação penal, ao tempo da prática do fato delituosa, é que serão consideradas como condutas típicas, e assim, serão punidas nos termos da lei.

4.1.2 Princípio da proibição de analogia em *malam partem*

Este princípio é decorrente do princípio da legalidade, pois não há crime nem pena sem lei estrita. Nas palavras de Damásio de Jesus (2010), esse princípio é "corolário da legalidade, proíbe a adequação típica 'por semelhança' entre fatos".

Ratificando esses termos, Julio Mirabete e Renato Fabbrini (2010, p. 41) ponderam que:

> Diante do princípio da legalidade do crime e da pena, pelo qual não se pode impor sanção penal a fato não previsto em lei, é inadmissível o emprego da analogia para criar ilícitos penais ou estabelecer sanções criminais.

Dessa maneira, não poderá ser o art.154-A ampliado o seu conceito para incriminar condutas não previstas expressamente na lei. Assim, esse princípio poderá ser utilizado em beneficio de quem invadir ativos lógicos virtuais capazes de armazenar dados e informações como uma rede social, disco virtual ou armazenamento em nuvem, ou mesmo um sistema de email virtual conhecido largamente por webmail.

No caso supracitado, ocorreu uma grave falha legislativa, ou mesmo uma omissão legislativa, haja vista, aqueles que tenham sua rede social devassada, mas sem a ocorrência da invasão de dispositivo informático alheio, não estarão resguardados pela Lei “Carolina Dieckmann”.

4.1.3 Princípio da anterioridade da lei

Também um princípio decorrente do princípio da legalidade, e que indica não haver crime nem pena sem definição de lei anterior, consagrado pelo brocardo *nullun crimen nulla poena sine lege praevia*. “Pelo princípio da anterioridade da lei penal (art. 1º), está estabelecido que não há crime sem lei anterior , o que configura a regra geral da irretroatividade da lei penal” (MIRABETE, FABBRINI, 2010, p. 43).

Assim, ninguém poderá ser punido por lei posterior a prática do fato delituoso. Pois, “para que haja crime e seja imposta pena é preciso que o fato tenha sido cometido depois de a lei entrar em vigor” (JESUS, 2010, p.51 e 52).

Comungando com os preceitos da obra de Rogério Greco (2010, p. 96 e 97), ao assegurar que:

> Além da necessidade inafastável da existência de uma lei proibindo ou impondo condutas sob a ameaça de sanção, é preciso que o agente tenha praticado o fato incriminado posteriormente à sua vigência. a lei, portanto, deve sempre estar em vigor anteriormente à conduta do agente. O marco, portanto, para que devamos obediência à lei penal, coo regra, é a data de sua vigência.

Assim, conforme a “teoria da ação, que considera praticado o crime no momento da ação ou omissão” (QUEIROZ, 2011, p. 108) só serão punidos os atos

praticados após o dia 2 de março do corrente ano, data esta, marcada pela entrada em vigor da Lei 12.737/2012.

4.1.4 Princípio da taxatividade

Mais um princípio dimensionada a partir do princípio da legalidade. O princípio da taxatividade segue a máxima *nullum crimem sine lege scripta et stricta*, ou seja, não haverá crime tampouco pena, sem lei certa.

Em sua obra, Rogério Sanches (2013, p. 82) traz os preceitos de Luiz Luisi (2003, p. 24) que afirma:

> Sem esse corolário o princípio da legalidade não alcançaria seu objetivo, pois de nada vale a anterioridade da lei, se esta não estiver dotada de clareza e da certeza necessárias, e indispensáveis para evitar formas diferenciadas, e, pois, arbitrárias na sua aplicação, ou seja, para reduzir o coeficiente de variabilidade subjetiva na aplicação da lei.

Não menos reluzente, Luiz Regis Prado, (2012, p.163) com o seu notável saber, elucida que:

> [...] Costuma-se a admitir uma distinção conceitual em razão do destinatário, em dois momentos, ora o do legislador, ora o do juiz. Através da determinação, exige-se que o legislador descreva da forma mais exata possível o fato punível. Diz respeito, em especial, à técnica de elaboração da lei penal, que deve ser suficientemente clara e precisa na formulação do conteúdo do tipo de injusto e no estabelecimento da sanção para que exista segurança jurídica. Desse modo, torna-se imperiosa para o Poder Legislativo a proibição de utilização excessiva e incorreta de elementos normativos, de casuísmos, cláusulas gerais e de conceitos indeterminados ou vagos na construção dos tipos legais de delito. Visa cumprir a exigência de certeza (*lex certa*), no sentido de que o conteúdo da lei possa ser conhecido por seus destinatários, permitindo-lhes diferenciar entre o penalmente lícito e o ilícito. Pela taxatividade, busca-se estabelecer as margens penais às quais está vinculado o julgador. Isso vale dizer: deve ele interpretar e aplicar a norma penal incriminadora nos limites estritos em que foi formulada, para satisfazer a exigência de garantia, evitando-se eventual abuso judicial. Em outras palavras, restringe-se a liberdade decisória do juiz

> (*arbitrium judicis*) a determinados parâmetros legais, que não podem ser ultrapassados no momento da aplicação da lei ao caso concreto. [...]

Este princípio é dirigido tanto ao legislador, delimitando na feitura das leis ao exigir que essas sejam precisas e claras, para que não deixem margens a possíveis dúvidas. Como também é destinado aos magistrados na aplicação da lei ao caso concreto, onde o juiz deve interpreta-la respeitando-se os limites estritos a que ela se propôs, garantindo-se uma segurança jurídica e restringindo-se a liberdade que juiz tem em sua decisão.

Com relação ao crime de invasão de dispositivo informático, o legislador não manteve a precisão que dele se espera, haja vista ser a lei passível de interpretações conflitantes. Certamente na aplicação ao caso concreto o magistrado ficará refém dessa confusa lei, pois o próprio termo “dispositivo informático” gera dúvida, não se sabe se a invasão terá que ser exclusivamente de um titular de um dispositivo. Nesse caso, aqueles que computadores de domínio público não estão protegidos com tal dispositivo. O mesmo termo também traz a incerteza de não se saber se redes sociais e computação em nuvem também serão tutelados pelo art. 154-A.

4.2 Crimes Por Meio de Um Computador e Internet

Anteriormente a entrada em vigor da Lei 12.737/2012, muitos crimes eram cometidos através de um dispositivo informático. Contudo, não é uma tarefa das mais fáceis a análise das condutas que se multiplicam pela internet, muito em virtude da dificuldade de encontrar o agente que praticou o delito, como também o pequeno número de decisões jurisprudências acerca desses delitos. Dentre os crimes utilizando-se o computador como meio estão, as fraudes virtuais, estelionato, invasão de privacidade, crimes contra a honra, entre outros.

4.2.1 Fraudes virtuais

Para o cometimento do crime em tela, o agente tem que praticar uma invasão, modificação ou supressão de dados eletrônicos ou programas, ou alguma outra forma que modifique a análise do processamento de dados. Assim, a ação tem como intenção obter dados e informações de pessoa física e jurídica, objetivando auferir algum tipo de vantagem, seja financeira, material ou mesmo psicológica.

Nesse caso, poderá se caracterizar um furto qualificado mediante fraude, conforme art. 155, § 4º, II, do Código Penal. Bem como a própria invasão de dispositivo informático, dependendo, é bem verdade, do caso concreto, pois neste caso o agente deverá invadir dispositivo informático alheio, conectado ou não a rede de computadores, mediante violação indevida de mecanismo de segurança.

Assim entende o TRF 4, em julgamento do HC 17675 do Rio Grande do Sul, publicado no portal Jusbrasil, no dia 27 de junho de 2007:

> PROCESSUAL PENAL. HABEAS CORPUS. PRISÃO PREVENTIVA. GARANTIA DA ORDEM PÚBLICA. FURTO QUALIFICADO (ART. 155 , § 4º , II , DO CP) E FORMAÇÃO DE QUADRILHA (ART. 288 DO CP). CRIMES PRATICADOSPELA INTERNET. 1. A gravidade dos crimes sob comento e a audácia das condutas, conduzem à necessidade da manutenção da prisão cautelar, no intuito de afastar do meio social o investigado, considerando que a atuação do paciente na quadrilha era intensa e figurava como um dos principais integrantes da trama delituosa, sendo essencial para o êxito dos delitos. 2. Presente a possibilidade de reiteração da conduta delituosa, uma vez em liberdade o paciente, tendo em conta se tratar de caso de crimes tecnológicos, de difícil rastreamento, praticado por hackers, altamente estimulados pelo desafio da praticar crimes sob o manto da impunidade, possuindo o conhecimento necessário à retomada das ações criminosas. (RIO GRANDE DO SUL, Tribunal Regional Federal da 4ª Região, HC 17675 RS 2007.04.00.017675-3, Relator: Tadaaqui Hirose, 2007).

4.2.2 Estelionato

Entre outros crimes cometidos através de um dispositivo informático, o estelionato é um dos mais praticados. Pois é um crime caracterizado pela obtenção para si ou para outrem, vantagem ilícita em prejuízo alheio, ao induzir ou manter alguém em erro mediante qualquer forma fraudulenta.

No caso de estelionato ser cometido através de um computador, ao obter dados e informações da vítima, mas que para isso tenha que mantê-la em erro mediante alguma forma fraudulenta, o agente criminoso tem a intenção de obter vantagem ilícita. Para que isso ocorra é necessário que o agente invada um dispositivo, burlando a sua segurança, como a finalidade de obter dados necessários para que se cometa o estelionato. Poderá também instalar vulnerabilidade a fim de obter vantagem ilícita.

Em julgamento do HC 49403 do Maranhão, o TRF 1 assim decidiu:

> PROCESSO PENAL. HABEAS CORPUS. ESTELIONATO. CRIMEPRATICADO PELA INTERNET. PRISÃO PREVENTIVA. INEXISTÊNCIA DOS REQUISITOS. 1. Crime de estelionato praticado pela internet, com a participação, segundo o que consta do inquérito, de diversas pessoas, com atuações determinadas - a) o programador (o que cria a página clone, os programas, ex. o Trojan ou cavalo de Tróia) - responsável pela captura da senha; é o cracker, não hacker, b) o usuário (o explorador direto do programa), ou seja, o operador do programa; c) o plaqueiro, (de placa), biscoiteiro ou cartãozeiro (responsável pela aquisição dos cartões bancários epela arrecadação de boletos que serão pagos via internet); d) sub-plaqueiro (a pessoa que, apesar de não conhecer os usuários do programa, compra os cartões magnéticos dos laranjas e os vende a plaqueiros que mantém contato com o usuário; e) o laranja (o que empresta sua conta para receber os créditos espúrios da internet) - com a finalidade de pescar (obter mediante ardil) a senha de correntistas [pishing = password (senha) + fishing (pescaria)] e retirar dinheiro de suas contas bancárias. 2. Se o paciente, segundo consta dos autos do inquérito, é mero laranja e sub-plaqueiro, dependendo sua atuação da do outros participantes do esquema, o programador e o usuário, não tem como perturbar a ordem pública, social, nem econômica, não havendo razão para que seja decretada sua prisão preventiva, como dito na decisão impugnada. (MARANHÃO, HC 49403 MA 2004.01.00.049403-5, Relator: Des. Tourinho Neto, 2004)

Uma das formas que esse tipo de crime pode ser cometido é através do envio de email contendo vírus que direcionam a vítima para um portal falso,

mantendo-a em erro, fazendo com que a vítima disponibilize informações suficientes para a obtenção de vantagem por parte do agente cometedor do delito. Não somente por possibilitar uma maior segurança na proteção dos dados contidos no dispositivo, mas, sobretudo para que o agente que comete o crime seja punido é necessário que o dispositivo informático esteja protegido por um antivírus. Só assim poderá ser caracterizado crime tipificado no art. 154-A do CP.

5 CONSIDERAÇÕES FINAIS

Devido à evolução informática juntamente com a globalização, a população tem presenciado inúmeros benefícios advindos com essa evolução. Contudo, muitos indivíduos se aproveitaram do anonimato e da incerteza na autoria para o cometimento de crimes. Muito em virtude dessa evolução tecnológica e consequente benefícios, as vendas de dispositivos informáticos cresceram, e, atualmente, estão presentes em todo lugar. Consequentemente, também houve o crescimento dos crimes virtuais ou crimes cibernéticos.

Esse crescimento na violação dos dispositivos fomentou a criação da Lei 12.737/2012, principalmente devido à comoção social causada pela invasão do dispositivo informático e obtenção de fotos pessoais da atriz global Carolina Dieckman. Devido à repercussão que o caso dessa atriz obteve, rapidamente os legisladores apresentaram o Projeto de Lei 35/2012, que deu origem a já supracitada Lei, e em pouco tempo esse projeto foi votado e aprovado.

Além do PL 35/2012 o PL 84/1999, aproveitando-se da força e pressão exercida pela mídia, também virou um dispositivo legal, que foi a Lei 12.735/2012. Tem como principal finalidade a estruturação dos órgãos da polícia judiciária com a finalidade de combater as ações delituosas em rede de computadores. Aqui é possível verificar que o último projeto passou mais de dez anos para ser votada.

Com isso foi ssível vislumbrar a presteza a ser realizada pelo Poder Legislativo que em certas ocasiões pratica a sua atividade típica, que é a feitura de leis, a partir de pressões realizadas através da mídia. Pressão que pode ser realizada diretamente, através dos meios jornalísticos, como também indiretamente, a partir de influências que a mídia realiza sobre a sociedade, e esta pressiona os legisladores.

Apesar de ser uma Lei que adveio por pressões externas, ela foi uma importante inovação legislativa. Anteriormente a ela não existia qualquer legislação tipificando a conduta de invadir dispositivo informático alheio, no qual passou a tutelar o direito a privacidade, bem como a intimidade e a vida privada. Nessa perspectiva, muitos foram a favor da criação deste tipo penal, pois a todo o momento os dispositivos eram devassados e nada era feito em relação ao agente que cometia o delito.

Contudo, especialistas no assunto fizeram diversas críticas acerca da Lei em comento. As críticas lançadas a baile vão desde a forma como a Lei foi criada, às pressas, como também, sobretudo, as realizadas a partir da análise e interpretação da tipificação penal. Haja vista, ter o legislador deixado brechas jurídicas, faltou a explicitação de alguns termos tecnicistas ou mesmo imprecisões jurídicas. Portanto, há mais dúvidas do que certezas, vindo a gerar problemas sérios.

Logo, as críticas foram voltadas desde o começo com o termo “invadir dispositivo informático alheio”, até o final do *caput* do art. 154-A, bem como o próprio preceito secundário, com reclusão de apenas três meses a um ano, e multa. Esse termo citado obteve relevantes contradições, pois não se sabe se os computadores de domínio público estarão abrangidos por esse termo. Também se questionou se as redes de armazenamento em nuvem estariam tuteladas pelo dispositivo ora em comento. Como visto, sem sombra de dúvidas, era para o legislador infraconstitucional ter delineado acerca dos termos técnicos presentes no tipo penal. Acreditando-se que o termo dispositivo informático se restringirá apenas aos hardwares (PC, notebook, smartphone, memórias externas), não foi abrangido o armazenamento em nuvem.

Outro termo duramente criticado é que para a configuração do crime de invasão de dispositivo se faz necessário que o mesmo esteja de alguma forma protegido, seja com senha pessoal, com antivírus, ou qualquer outro tipo de proteção. Assim, se um indivíduo deixa o computador sem antivírus ou deixa-o aberto, e o agente nele se instala, este não cometeu nenhum crime, pois o dispositivo está desprotegido. Mesmo que o a conduta seja a de invadir o dispositivo, sem o consentimento da vítima, para obter, adulterar ou destruir dados ou informações, não estando sob algum mecanismo de segurança, não resta outra solução senão a atipicidade da conduta.

Outro termo questionado é com relação à instalação de vulnerabilidade, pois para adentrar no dispositivo informático é necessário que o agente viole mecanismo de segurança, ao violar esse mecanismo, o delinquente estará explorando algum tipo de vulnerabilidade. Assim, torna a expressão um tanto quanto imprópria, haja vista ter o agente que invadir o dispositivo, explorando uma vulnerabilidade do mecanismo de segurança, para instalar uma vulnerabilidade.

Também cabe ressaltar que o preceito secundário ficou aquém do necessário, haja vista, ter sido previsto uma pena de reclusão de três meses a um

ano e multa. Sendo a ação penal pública condicionada a representação, o aparelhamento da polícia judiciária ser defasado, juntamente com a baixa pena em abstrato, ocorrerão inúmeros casos que ficarão prescritos, ocasionando a impunidade.

Diante de todo o exposto, no presente estudo, vislumbrou-se que não adiantam a feitura de novas leis quando estas são mal elaboradas. Muito embora seja necessário a tipificação de algumas condutas, na tentativa de coibi-las, não será sempre que isso ocorrerá. Nos últimos anos, muitos delitos foram criados e nem por isso diminuiu-se a criminalidade. Desse modo, o que se espera dos legisladores é a criação de leis com qualidade, e não quantidade.

REFERÊNCIAS

BITENCOURT, Cezar Roberto. Invasão de dispositivo informático. **Atualidades do Direito**. Disponível em: <http://atualidadesdodireito.com.br/cezarbitencourt/2012/12/17/invasao-de-dispositivo-informatico/>. Acesso em: 20 de agosto de 2013.

BLANC, Antonio. Conheça a história de quase meio século dos tablets. **Terra**. Disponível em: <http://tecnologia.terra.com.br/hardware-e-software/conheca-a-historia-de-quase-meio-seculo-dos-tablets,9c08fc67b84ea310VgnCLD200000bbcceb0aRCRD.html>. Acesso em: 1 de agosto de 2013.

BRASIL, Câmara Federal. Projeto de Lei n° 84/99. **Dispõe sobre os crimes cometidos na área da informática, suas penalidades e dá outras providências**. Disponível em: <http://www.camara.gov.br/sileg/Prop_Detalhe.asp?id=15028>. Acesso em: 18 de agosto de 2013.

_____. Câmara Federal. Projeto de Lei n° 35/2012. **Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências**. Disponível em: <http://www.senado.gov.br/atividade/materia/detalhes.asp?p_cod_mate=105612> Acesso em: 18 de agosto de 2013.

_____. **Constituição da República Federativa do Brasil**, 05 de outubro de 1988. Diário Oficial da União. Brasília, 05.out.1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 30 de julho de 2013.

_____. Decreto-lei n° 2.848, de 07 de dezembro de 1940. **Código Penal**. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_ato20112014/2012/lei/l12737.htm> Acesso em: 25 de julho de 2013.

_____. Tribunal Regional Federal da 1ª Região. Habeas Corpus nº 49.403/MA 2004.01.00.049403-5. Relator: Des. Tourinho Neto. Julgamento em: 22 de novembro de 2004. Disponível em: <http://trf-1.jusbrasil.com.br/jurisprudencia/2249562/habeas-corpus-hc-49403-ma-20040100049403-5>. Acesso em: 3 de setembro de 2013.

_____. Tribunal Regional Federal da 4ª Região. Habeas Corpus nº 17.675/RS 2007.04.00.017675-3. Relator: Tadaaqui Hirose. Julgamento em: 19 de junho de 2007. Disponível em: <http://trf-4.jusbrasil.com.br/jurisprudencia/1254042/habeas-corpus-hc-17675>. Acesso em: 3 de setembro de 2013.

BULOS, Uadi Lammego. **Constituição Federal Anotada**. 7. ed. rev. atual. São Paulo: Saraiva, 2007.

CABETTE, Eduardo Luiz Santos. O novo crime de Invasão de Dispositivo Informático. **Consultor Jurídico**. Disponível em: <http://www.conjur.com.br/2013-fev-04/eduardo-cabette-crime-invasao-dispositivo-informatico>. Acesso em: 20 de agosto de 2013.

CANTÚ, Evandro. **Redes de Computadores e Internet**. São José: Primavera, 2003.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 4.ed. São Paulo: Saraiva, 2008.

CRUZ, Danielle da Rocha Cruz. **Criminalidade Informática Tipificação Penal das Condutas Ilícitas Realizadas com Cartão de Crédito**. Rio de Janeiro: Forense, 2006.

CUNHA, Rogério Sanches. **Manual de Direito Penal Parte Geral**. V. Único. Salvador: Juspodivm, 2013.

_____. **Manual de Direito Penal Parte Especial**. V. Único. 5. ed. rev. amp. atual. Salvador: Juspodivm, 2013.

GOMES, Adão Mendes. A Inclusão do Homicídio como Crime Hediondo. **O Direito na Berlinda**. Disponível em: <http://adaomendesdireitouneb.blogspot.com.br/2012/03/inclusao-do-homicidio-como-crime.html>. Acesso em: 20 de agosto de 2013.

GRECO, Rogério. **Curso de Direito Penal, Parte Geral,** V. I. 12.ed. Niteroi: Impetus, 2010.

_____. **Curso de Direito Penal, Parte Especial**. V. II. 7. Ed. Niteroi: Impetus, 2010.

_____. Invasão De Dispositivo Informático – Art. 154-A Do Código Penal. **Atualidades do Direito**. Disponível em: <http://atualidadesdodireito.com.br/rogeriogreco/2013/01/08/invasao-de-dispositivo-informatico-art-154-a-do-codigo-penal/>. Acesso em: 22 de agosto de 2013.

INTEL BRASIL, **Pesquisa da Intel mapeia a penetração de computadores e internet nos lares brasileiros**, 2011. Disponível em: <http://newsroom.intel.com/community/pt_br/blog/2011/09/27/pesquisa-da-intel-mapeia-a-penetra%C3%A7%C3%A3o-de-computadores-e-internet-nos-lares-brasileiros>. Acesso em: 25 de julho de 2013.

JESUS, Damásio E. de. **Direito Penal Parte Geral**. V. 1. 31. ed. São Paulo: Saraiva, 2010.

MAGGIO, Vicente de Paula Rodrigues. Novo Crime: Invasão De Dispositivo Informático – Cp, Art. 154-A. **Atualidades do Direito**. Disponível em: <http://atualidadesdodireito.com.br/vicentemaggio/2012/12/16/invasao-de-dispositivo-informatico-cp-art-154-a/>. Acesso em: 22 de agosto de 2013.

MIRABETE, Julio Fabbrini; FABBRINI, Renato N. **Manual de Direito Penal, Parte Geral, Arts. 1º a 120 do CP**, V. I. 26. ed. rev. atual. São Paulo: Atlas 2010.

MOURA, Pâmela Aline Rocha. **Crime Cibernético e Seus Aspectos no Universo Jurídico**. Barbacena: UNIPAC, 2012.

NOVELINO, Marcelo. Direito Constitucional. 6. Ed. rev. atual. ampl. São Paulo: Método, 2012.

NUCCI, Guilherme de Souza. **Código Penal Comentado**. 11. Ed. rev. atual. ampl. São Paulo: Revista dos Tribunais, 2012.

PIMENTEL, Alexandre Freire. **O Direito Cibernético Um Enfoque Teórico e Lógico-Aplicativo**. Rio de Janeiro: Renovar, 2000.

PRADA, Rodrigo. A História dos Notebooks, **Tecmundo**. Disponível em: < www.tecmundo.com.br/2231-a-historia-dos-notebooks.htm>. Acesso em: 28 de julho de 2013.

PRADO, Luiz Regis. **Curso de Direito Penal Brasileiro, Parte Geral – Arts. 1º a 120**. V. 1. 11.ed. São Paulo: Revista dos Tribunais, 2012.

PRECE, Da France. Número de usuários de internet no mundo alcança os 2 bilhões. G1. Disponível em: <http://g1.globo.com/tecnologia/noticia/2011/01/numero-de-

usuarios-de-internet-no-mundo-alcanca-os-2-bilhoes.html>. Acesso em: 8 de agosto de 2013.

QUEIROZ, Paulo. **Direito Penal Parte Geral**. 7.ed. Rio de Janeiro: Lumen Juris, 2011.

SAMPAIO, Luciano de. A História dos Tablets. **Tecmundo**. Disponível em: <http://www.tecmundo.com.br/3624-a-historia-dos-tablets.htm>. Acesso em: 30 de julho de 2013.

SIENA. David Pimentel Barbosa de Siena. Lei Carolina Dieckmann e a definição de "crimes virtuais". **Jus Navigandi**. Disponível em: <http://jus.com.br/artigos/24406/lei-carolina-dieckmann-e-a-definicao-de-crimes-virtuais/1>. Acesso em: 25 de agosto de 2013.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 30. Ed. São Paulo: Malheiros, 2008.