UNIVERSIDADE DO SUL DE SANTA CATARINA

GABRIELA APARECIDA EUZÉBIO

O CRIME DE INVASÃO DE DISPOSITIVO INFORMÁTICO ACRESCIDO PELA "LEI CAROLINA DIECKMANN" SOB A PERSPECTIVA DO PRINCÍPIO DA PROPORCIONALIDADE

Içara

2014

GABRIELA APARECIDA EUZÉBIO

O CRIME DE INVASÃO DE DISPOSITIVO INFORMÁTICO ACRESCIDO PELA "LEI CAROLINA DIECKMANN" SOB A PERSPECTIVA DO PRINCÍPIO DA PROPORCIONALIDADE

Monografia apresentada ao Curso Direito da Universidade do Sul de Santa Catarina, como requisito parcial à obtenção do título de Bacharel em Direito.

Linha de pesquisa: Justiça e Sociedade

Orientadora: Profª. Madilini Mariáh Külkamp Gurgacz, Esp.

Içara

2014

GABRIELA APARECIDA EUZÉBIO

O CRIME DE INVASÃO DE DISPOSITIVO INFORMÁTICO ACRESCIDO PELA "LEI CAROLINA DIECKMANN" SOB A ÓTICA DO PRINCÍPIO DA PROPORCIONALIDADE

Esta monografia foi julgada adequada à obtenção do título de Bacharel em Direito e aprovada em sua forma final pelo Curso de Direito da Universidade do Sul de Santa Catarina.

Içara, 26 de junho de 2014.

_____

Profª. e orientadora Madilini Mariáh Külkamp Gurgacz, Esp.
Universidade do Sul de Santa Catarina

_____

Prof. Ronaldo da Silva Cruz, Esp.
Universidade do Sul de Santa Catarina

_____

Prof. Bruno De Farias Favaro, Esp.
Universidade do Sul de Santa Catarina

Dedico este trabalho aos alicerces da minha vida: meu sublime Deus, por estar presente em todos os momentos e à minha amada família, em especial aos meus pais Sérgio e Claudeci, que me ensinaram a ser a pessoa que sou hoje.

AGRADECIMENTOS

Agradeço a Deus, pelo dom da vida, pelo seu cuidado e amor incondicional. Sem Ele, nada sou.

À minha família, que foi, é e sempre será meu porto seguro. Minha mãe, Claudeci, meu pai, Sérgio, e meu irmão Juliano, vocês são os maiores motivos de eu ter me empenhado para chegar até aqui. Sou grata pelo amor, incentivo e dedicação de vocês. Pelas orações em meu favor e pela preocupação para que eu estivesse sempre andando pelo caminho correto. Obrigada por terem acreditado em mim e por serem a melhor e mais digna plateia das minhas conquistas.

Aos amigos de perto e de longe, pelo amor e preocupação. Natanael e Saudi, essa conquista eu compartilho com vocês, com muita alegria, pois vocês participaram tão de perto de todo esse momento que tenho vivido. Vocês também fazem parte desta vitória.

Aos professores da Unisul, que muito contribuíram para minha formação e em especial à professora e amiga Madilini, pela ajuda desde a escolha do tema, pela disposição, carinho e apoio, bem como por ter dedicado do seu tempo para me orientar neste trabalho.

Aos colegas de classe, que me acompanharam neste percurso acadêmico. Em especial à Rosilaine, Clarissa, Thays e Fernando, por todo apoio e cumplicidade nestes cinco anos de graduação.

Sou grata também a todas as pessoas que fizeram parte da minha caminhada profissional até o presente momento, dentre as quais destaco os colegas de trabalho, Advogados, Juízes, Promotores e demais profissionais do Direito com os quais eu pude ter contato direto durante esse tempo. Espelho-me em vocês a cada dia.

Agradeço ao Doutor Júlio César Bernardes, Juiz de Direito, por ter aberto as portas da magistratura, a fim de que eu pudesse experimentar na prática as virtudes dessa carreira brilhante.

Em especial ao Doutor Luiz Henrique Bonatelli, cujo exemplo de pessoa ultrapassam os limites de um magistrado: conduta, caráter e seriedade. Foi uma honra trabalhar com o Senhor.

Também ao magistrado Fernando Dal Bó Martins, pela paciência, suporte e pelos ensinamentos transmitidos ao longo desse tempo.

Sou grata a todos que, direta ou indiretamente, contribuíram para a realização deste trabalho, a todos que acreditaram em mim e sempre me apoiaram.

“A lei é inteligência, e sua função natural é impor o procedimento correto e proibir a má ação”. (CÍCERO).

RESUMO

Nesta pesquisa, procurou-se avaliar a importância dos denominados crimes informáticos, demonstrando ser imprescindível a sua tutela pelo Direito Penal. Desta forma, discorreu-se acerca das recentes alterações promovidas pela Lei n. 12.737/2012 ("Lei Carolina Dieckmann"), sobretudo da nova tipificação do crime de "Invasão de dispositivo informático" (CP, art. 154-A), a qual foi enfoque do presente estudo. Além disso, discutiu-se a respeito das penas cominadas do aludido artigo e, ainda, sua relação de pertinência com a gravidade das condutas praticadas pelo agente e suas consequências, apresentando assim uma problemática com relação ao princípio da proporcionalidade. A justificativa para o presente trabalho foi, além de expor o dissabor pela má redação do artigo 154-A do Código Penal, acrescido pela Lei n. 12.737/2012, também demonstrar a inobservância do princípio da proporcionalidade pelo legislador penal no momento da cominação das penas. O método de abordagem para a pesquisa foi o dedutivo. O método de procedimento, por sua vez, foi o monográfico, utilizando se a pesquisa documental e bibliográfica. O nível de pesquisa utilizado foi o explicativo e a abordagem, qualitativa. Os resultados foram satisfatórios, ao demonstrar que, por vezes, o legislador penal não respeita as diretrizes de princípios constitucionais, tal como o princípio da proporcionalidade, no momento em redigir a norma penal, resultando assim em leis vagas, imprecisas e ambíguas. Isso acontece, geralmente, pelo imediatismo penal que tem vivenciado o país atualmente, o qual é resultado da pressão imposta pela mídia que rotineiramente celebriza determinados acontecimentos. O princípio da proporcionalidade é, então, de extrema importância para a correta e justa elaboração da norma penal.

Palavras-chave: Crimes informáticos. Lei Carolina Dieckmann. Invasão de dispositivo informático. Proporcionalidade. Atividade legiferante.

ABSTRACT

In this research, was sought to avalue the importance of the called computer crime, showing be necessary its guardianship by Criminal Law. This way, was wrote about the recent changes promoted by Law n. 12.737/2012 (“Carolina Dieckmann Law”), above all the new crime typing like "Informatic Device Invasion" (CP, art. 154-A), which was focus of the present study. Moreover, was discussed about imposed sentences of alluded article and, yet, it relevance relation with practice conduct gravity, showing a problematic about principle of proportionality. The justify to the present work was, behind expose the disappointment with article 154-A of Criminal Code's bad writing, added by Law n. 12.737/2012, also demonstrate the non-observance the principle of proportionality by criminal lawmaker at the criminal impose's moment. The approach method for the research was the deductive. The procedure method, by the time, was the monographic, using the document and bibliographic research. The research level used was explanatory and approach, was qualitative. The results were satisfying, demonstrating that, by the times, the criminal lawmaker don't respect constitutional principles guidelines, such as the principle of proportionality, at the moment of writing criminal standard, resulting on empty, inaccurate and double laws. It usually happens, by the criminal immediacy that country has living currently, whose is resulted of imposed pression by media that routinaly focus certains events. The principle of proportionality is therefore of extreme matter for correct and fair making of criminal standard.

Key-words: Computer crimes. Carolina Dieckmann Law. Informatic device invasion. Proportionality. Lawmaker activity.

LISTA DE ABREVIATURAS E SIGLAS

§ – parágrafo

AI-5 – Ato Institucional Número 5

ARPANET – *Advanced Research Projects Agency*

art. – artigo

CF/88 – Constituição Federal da República de 1988

CP – Código Penal

CPU (*Central Processing Unit*) – Unidade de processamento de dados

EUA – Estados Unidos da América

FTP (*File Transfer Protocol*) – Protocolo de transferência de arquivos

IP – *Internet Protocol*

PC – (*Personal Computer*) – Computador pessoal

PL – Projeto de lei

STF – Supremo Tribunal Federal

STJ – Superior Tribunal de Justiça

SUMÁRIO

1 INTRODUÇÃO

Estamos vivenciando a era da sociedade digital. Hodiernamente, a utilização de dispositivos informáticos, notadamente o computador, torna-se imprescindível, pois tal ferramenta é utilizada praticamente em todas as ações do cotidiano, seja por instituições públicas ou privadas. As relações pessoais também sofreram grandes impactos com o advento do computador e com a popularização das redes sociais.

Paralelamente ao avanço tecnológico, surgem as novas práticas delituosas, seja como modo alternativo de obtenção indevida de riquezas, seja no intuito – simplesmente – de causar danos a outrem. Talvez, em razão disso, recentemente emergiram grandes debates entre os operadores de direito acerca dos denominados "crimes informáticos". É certo que o Código Penal (BRASIL, 1940) e as legislações penais esparsas se revelam insuficientes para tutelar essas novas práticas delituosas no campo da informática.

Com efeito, é oportuno ressaltar que o forte clamor público manifestado por intermédio dos meios de comunicação, principalmente após a repercussão do episódio ocorrido pela atriz Carolina Dieckmann, em 2012, acabou por influenciar a rápida aprovação de projetos de lei sobre o tema que já tramitavam no Congresso há tempo considerável. Nesse contexto, surge a Lei n. 12.737 (BRASIL, 2012), intitulada com o nome da referida atriz que, alterando o Código Penal (BRASIL, 1940), tipificou a conduta de "Invasão de dispositivo informático" (CP, art. 154-A).

No entanto, o aludido dispositivo penal foi alvo de numerosas críticas por parte dos mais diversos operadores de direito que questionavam seus efeitos jurídicos e sua aplicabilidade no campo prático. A propósito disso, entende-se que o novo tipo penal em questão apresenta uma redação ambígua e complexa, deflagrando inúmeras dúvidas entre aqueles que dela se utilizam. Acresce-se a isso o fato de que, numa primeira análise, é simples perceber que a pena cominada no artigo 154-A do Código Penal é um tanto quanto ínfima, quando sobpesada com a gravidade e as consequências dos crimes informáticos. (BRASIL, 1940).

Esse quadro leva à necessidade de se refletir, de forma crítica, acerca da criação do tipo penal em comento, bem como questionar a atuação do Poder Legislativo que, na maior parte das vezes, edita diplomas legais ao bel prazer dos veículos de comunicação, sem se preocupar com a tecnicidade jurídica e com os reflexos que a norma possa produzir no mundo fático.

1.1 DELIMITAÇÃO DO TEMA E FORMULAÇÃO DO PROBLEMA

Os recentes avanços tecnológicos aliados à ampliação ao acesso aos microcomputadores trouxeram impactos significativos para a sociedade contemporânea. A internet tornou-se, em um curto espaço de tempo, um meio de comunicação indispensável da era globalizada.

Entretanto, as consequências diretas desse avanço (o uso demasiado dos microcomputadores e o forte crescimento na utilização da rede mundial de computadores) proporcionaram mudanças não só positivas, como também negativas, na medida em que proporcionaram o desenvolvimento de novas práticas delituosas: os denominados crimes informáticos.

É válido dizer que, para os crimes cometidos por meio da internet, tais como fraude, furto, estelionato e crimes contra a honra, a legislação já existente em nosso ordenamento jurídico foi capaz, num primeiro momento, de resguardar a tutela desses interesses jurídicos, considerando a previsão legal de tais condutas no Código Penal Brasileiro. (BRASIL, 1940).

À medida que o acesso à internet foi crescendo, assim como os aparelhos informáticos e os programas de computadores foram se modernizando, novos delitos foram recrudescendo de forma inovadora e inesperada. Percebeu-se, então, que para novas práticas conhecidas como dano informático, violação ao dispositivo informático, ou mesmo invasão ao dispositivo informático, o Código Penal Brasileiro (BRASIL, 1940) e a legislação extrapenal até então vigente, revelavam-se insuficientes para coibir tais práticas.

Frente a isso, é importante esclarecer que, até então, eventuais danos advindos do uso indevido do acesso à informação através da internet vinham sendo solucionados na esfera cível, seja por meio de ações indenizatórias ou por meio de fixação de medidas urgentes/acautelatórias, como, por exemplo, a remoção de uma notícia ou imagem ofensiva da rede mundial de computadores.

Todavia, o cenário atual mostra que a reparação dos danos na seara cível, isoladamente, não é o bastante para dirimir a prática de tais delitos. Sobre este aspecto, cabe trazer à tona o fato veiculado pelos jornais e pela televisão ocorrido com a atriz global, Carolina Dieckmann, no qual trinta e seis fotos da atriz nua foram extraídas e indevidamente divulgadas na internet.

A citada atriz recebeu pelo menos três telefonemas e quatro ou cinco *e-mails* de um “chantageador”, que cobrava a quantia de R$ 10 mil para que as imagens não fossem

divulgadas. A suspeita é de que as imagens foram "roubadas" do computador da atriz há dois meses, quando ela levou o equipamento para manutenção (BORGES; WENECK, 2012). O caso ganhou destaque nos jornais e na televisão e, curiosamente, a problemática dos crimes cibernéticos - que apesar de já ser alvo de discussão no âmbito legislativo há mais de 17 anos -, subitamente, pelo alarde da mídia, despertou o interesse dos membros do parlamento.

Assim, no afã de dar uma resposta imediatista à sociedade impactada pela mídia, foi publicada em 03 de dezembro de 2012, através do Diário Oficial da União, a Lei n. 12.737 (BRASIL, 2012), também conhecida como "Lei Carolina Dieckmann", que, além de prever algumas condutas para os crimes informáticos, alterou alguns dispositivos já previstos no Código Penal Brasileiro. (BRASIL, 1940).

Como se vê, tal episódio serviu de estopim para que os legisladores alertassem para a necessidade de criação de mecanismos jurídicos direcionados a prevenção e repressão dessa nova forma de criminalidade, caracterizada, sobretudo, pelo alto grau de tecnicidade e especialização. Um desses mecanismos foi a criação do tipo penal previsto no artigo 154-A, inserido no capítulo dos crimes contra a liberdade individual do Código Penal de 1940, com a seguinte redação:

> 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, governador 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. (BRASIL, 1940, grifo meu).

Nesse viés, menciona-se o princípio da proporcionalidade, o qual tem sido reconhecido tanto doutrinariamente quanto jurisprudencialmente, tornando-se, portanto, indispensável na atividade legiferante, sobretudo no âmbito penal. Diante desse quadro, fica o questionamento: As penas cominadas no artigo 154-A, criado com a Lei n. 12.737/2012 (“Lei Carolina Dieckmann”), atendem ao princípio da proporcionalidade?

1.2 JUSTIFICATIVA

Objeto de embates, a famigerada Lei n. 12.737 (BRASIL, 2012) tem sido discutida pelos diversos juristas atuantes das áreas de Direito Penal e Direito Eletrônico, sobretudo sobre sua (in) aplicabilidade prática.

É cediço que a prática de crimes informáticos tem se tornando algo cada vez mais rotineiro no Brasil, de maneira que houve uma necessidade de se tentar prevenir os resultados advindos destes crimes, bem como sancionar os criminosos que atuam nessa área por suas atuações.

Para tanto, publicou-se uma lei, a qual se popularizou como “Lei Carolina Dieckmann” com o intuito de solucionar - ainda que de forma parcial - os problemas ocasionados por essa prática ilícita não amparada pela legislação penal até então vigente. Anota-se, contudo, que o tipo penal trazido pela Lei n. 12.737/2012 possui uma redação ambígua e cercada de brechas. Além disso, contém uma pena insuficiente, uma vez que é incapaz de causar intimidação aos praticantes do crime de “Invasão de dispositivo informático”. (BRASIL, 2012).

À vista disso, a atualidade da legislação brasileira referente aos crimes informáticos, aliada à afinidade com a ciência do Direito Penal justificou, num primeiro momento, a escolha do presente tema. Mas não somente isso. Mais do que expor o dissabor ocasionado pela má redação da Lei n. 12.737/2012 (sobretudo da norma acrescida, sob a forma do artigo 154-A), a intenção maior do presente estudo é demonstrar no decorrer destas linhas a inobservância do princípio da proporcionalidade pelo legislador penal no momento da cominação das penas. (BRASIL, 2012).

Assim, é inegável a relevância deste tema, pois busca-se esclarecer acerca das lacunas deixadas pelo legislador na redação do referido tipo penal, oportunizando assim uma reflexão crítica a respeito do cenário no qual as leis penais incriminadoras são editadas no país.

1.3 OBJETIVOS

1.3.1 Geral

Analisar a redação do tipo penal “Invasão de dispositivo informático” (CP, art. 154-A) acrescido ao Código Penal pela “Lei Carolina Dieckmann” sob a perspectiva do princípio da proporcionalidade.

1.3.2 Específicos

Para atingir o objetivo geral, foram formulados os seguintes objetivos específicos:

- discorrer acerca da evolução dos chamados crimes informáticos e da necessidade de se tipificar novas condutas não amparadas no ordenamento jurídico vigente;
- demonstrar a necessidade de tutela jurídica aos dados e informações armazenados em ambiente informático, os quais se encontram cada vez mais vulneráveis à ataques de criminosos;
- analisar a redação da tipificação do artigo 154-A do Código Penal de 1940, verificando as possíveis lacunas deixadas pelo legislador;
- verificar as diferentes interpretações acerca do referido tipo penal realizadas pelos operadores de direito;
- averiguar se as penas cominadas para a conduta de invadir dispositivo informático obedecem aos elementos do princípio da proporcionalidade: adequação, necessidade e proporcionalidade em sentido estrito;
- comentar, brevemente, acerca da atual estrutura e recursos existentes, no país, no tocante à investigação e apuração dos crimes informáticos;
- refletir de forma crítica acerca da realidade que envolve a edição das leis brasileiras, as quais crescem em ritmo acelerado no Brasil, sobretudo sobre a influência da mídia na produção legislativa penal brasileira.

1.4 PROCEDIMENTOS METODOLÓGICOS

No sentido de viabilizar um suporte teórico que proporcionasse bases consistentes de análise, adotou-se o método dedutivo que, nos dizeres de Motta (2012, p. 86), é aquele que

"origina-se das teorias e leis para predizer a ocorrência dos fenômenos particulares".

Quanto aos procedimentos técnicos, foi utilizada a pesquisa bibliográfica, no intuito de se obter, com base em material já elaborado, constituído principalmente de livros e artigos científicos, a análise de aspectos relevantes do tema, almejando, assim, uma pesquisa detalhada do conteúdo proposto.

Ainda, para a elaboração do presente trabalho, empregou-se a pesquisa documental, fazendo-se uso de doutrinas, notícias em jornais e sítios e leis específicas sobre o tema. Segundo Gil (2008, p. 51), a pesquisa documental "vale-se de materiais que não receberam ainda um tratamento analítico, ou que ainda podem ser reelaborados de acordo com os objetivos da pesquisa".

Quanto à abordagem, esta foi qualitativa, a qual, na visão de Gil (2008), procura dar respostas aos aspectos da realidade que não podem ser quantificados. Já no que tange ao nível de pesquisa, este foi o explicativo, uma vez que o presente trabalho, além da análise do conteúdo do tipo penal acrescido pela Lei n. 12.737 (BRASIL, 2012), visou à verificação da sua consonância com o princípio da proporcionalidade.

1.5 DESENVOLVIMENTO DO TRABALHO: ESTRUTURAÇÃO DOS CAPÍTULOS

O presente trabalho monográfico foi estruturado de maneira que fossem atendidas as questões referentes aos objetivos geral e específicos. Num primeiro momento, procurou-se apresentar as atuais vulnerabilidades em ambiente informático, sobretudo as formas mais comuns de invasão, utilizadas geralmente por intermédio da rede de computadores e, ainda, alguns mecanismos de segurança usualmente utilizados pelos usuários, objetivando a prevenção de ataques em meio informático. Tais informações foram essenciais para um melhor entendimento da redação do tipo penal de invasão de dispositivo informático.

Em seguida, buscou-se mostrar as consequências provenientes do avanço tecnológico para o meio jurídico, principalmente no que dizem respeito aos chamados crimes informáticos.

Tecidas tais considerações, passou-se à abordagem das questões relativas à tutela jurídico-penal dos crimes informáticos, mormente da necessidade de se tipificar novas condutas que não eram protegidas pela legislação penal vigente. Na sequência, apresentaram-se os projetos de leis que originariamente tratavam do tema até chegar ao novo tipo penal acrescido ao Código Penal (BRASIL, 1940) pela lei n. 12.737/2012: "Invasão de dispositivo informático".

No quarto capítulo, passou-se a explanar acerca do princípio da proporcionalidade, notadamente sobre sua aplicação pelo legislador penal no momento da elaboração das normas e suas respectivas penas.

No último capítulo, analisou-se a redação do artigo 154-A do Código Penal (invasão de dispositivo informático), verificando se os critérios utilizados pelo legislador pátrio no momento da elaboração da norma penal e sua respectiva pena atenderam ao princípio da proporcionalidade. (BRASIL, 1940).

Ao final, foi feita uma breve análise crítica acerca da realidade que envolve a edição das leis no ordenamento jurídico, levando-se em consideração todo o estudo abordado nos capítulos anteriores.

2 NOÇÕES GERAIS DE SEGURANÇA DA INFORMAÇÃO VIRTUAL E CRIMES INFORMÁTICOS

Preliminarmente, antes de adentrar o estudo da Lei n. 12.737/2012, popularmente conhecida como “Lei Carolina Dieckmann” (BRASIL, 2012), é interessante tecer breves comentários sobre a internet e sobre o avanço da tecnologia e suas consequências para o mundo jurídico. Necessário, também, definir o que vem a serem os chamados crimes informáticos, sua classificação, e a situação em que se encontram nos dias atuais.

Ademais, é indispensável explicitar a importância da chamada segurança da informação, a fim de auxiliar na compreensão das diversas ameaças existentes hoje no meio informático, bem como definir alguns termos essenciais utilizados em ambiente informático. Devido ao fato desta área possuir expressões terminológicas próprias é necessário fazer a leitura destas expressões, uma vez que somará ao melhor entendimento da temática abordada no presente trabalho.

2.2 INTERNET E TECNOLOGIA

Com a humanidade vivenciando o auge do crescimento tecnológico, é visível o quanto as pessoas estão envolvidas com o que se denomina hoje de internet. Ela se tornou de fato uma ferramenta profissional e pessoal indispensável no cotidiano das pessoas.

Conforme salientam Laudon e Laudon (2007, p. 178), a internet se tornou, nos últimos anos, o sistema de comunicação público mais abrangente, sendo considerada o maior exemplo de redes interconectadas e computação cliente/servidor no planeta, conectando centenas de milhares de redes individuais em todo o mundo.

Para explicitar melhor o crescimento da Rede, basta comparar a expansão da telefonia e a da *Web*; enquanto aquela demorou setenta e quatro anos para atingir o número de 50 milhões de usuários, esta demorou tão somente quatro anos para atingir o mesmo número. (BATISTA, 2006, p. 70).

Tal revolução causada pela internet é compreensível: a informação trocada entre os usuários, o fácil acesso aos conteúdos de imagens e vídeos, as conversas *on-line*, o acesso à Rede por meio de computadores ou mesmo *smartphones* tornaram as informações mais rápidas a serem divulgadas.

Nesse contexto, tanto as pessoas físicas quanto jurídicas tornaram a Rede Mundial de Computadores o seu meio de comunicação, negociação, propagação de informações como

também banco de dados virtuais, incluindo também os dispositivos capazes de armazenar arquivos e informações sem estarem conectados necessariamente à Rede, mas podendo também trocar informações entre si de forma direta.

2.1.1 Conceito de internet

Popularmente conhecida como "A Rede Mundial de Computadores", Tanenbaum (2003, p. 53) afirma que "a *internet* não é de modo algum uma rede, mas sim um vasto conjunto de redes diferentes que utilizam certos protocolos comuns e fornecem determinados serviços comuns".

De forma sucinta, Batista (2006, p. 70) a define como sendo uma interligação de várias redes em todo o mundo, utilizando os mesmos padrões de comunicação, resultando em uma revolução nas telecomunicações.

Laudon e Laudon (2007, p. 178) asseveram que "a palavra *Internet* deriva de *internetworking*, ou seja, a ação de conectar redes separadas, cada uma das quais retendo sua própria identidade, em uma rede interconectada".

Nas palavras de Rosa (2006, p. 35),

> [...] a *Internet* consiste num conjunto de tecnologias para acesso, distribuição e disseminação de informação em redes de computadores. A rede é o compartilhamento de informações e serviços. Um trabalho em rede é possível quando pessoas ou grupos possuem informações ou serviços que desejam compartilhar. Pode-se dizer, portanto, que a *Internet* é um conjunto de redes de computadores interligados pelo mundo inteiro, que têm em comum um conjunto de protocolos e serviços, possuindo a peculiaridade de funcionar pelo sistema de trocas de pacotes, ou seja, as mensagens dividem-se em pacotes e cada pacote pode surgir uma rota distinta para chegar ao mesmo ponto.

Ademais, faz-se importante mencionar que a recente lei n. 12.965/2014, popularizada como sendo o Marco Civil da Internet, definiu internet como sendo "o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes". (BRASIL, 2014, art. 5º, inciso I).

Feita essa consideração terminológica, passa-se a tecer importantes considerações a respeito da evolução histórica dos computadores e, por consequência, da internet.

2.1.2 Evolução histórica

Seria impossível falar de internet e crimes informáticos sem antes, contudo, adentrar na evolução histórica da informática, sobretudo do computador, ferramenta que revolucionou o conceito de comunicação.

O computador foi criado em meados da Segunda Guerra Mundial, para fins de processamento de dados. Era utilizado para calcular a tabela de artilharia para cada lote de munição que fosse fabricado, propiciando, desta forma, o controle de estoque dos materiais bélicos. (MAZZARDO; GÖSSLING, 2013).

Os primeiros computadores eram de grande porte e relativamente caros, levando-se em consideração a capacidade de processamento que dispunham. Desta forma, apenas as grandes empresas e poucas universidades conseguiam instalar essas gigantescas máquinas, as quais necessitavam, obrigatoriamente, de um espaço grande e refrigerado.

Foi a partir da década de 60 que vários usuários puderam compartilhar o uso de um mesmo computador. Os usuários se comunicavam a uma CPU (*Central Processing Unit*) e executavam seus programas por meio de seus terminais. Os computadores pessoais, popularmente conhecidos como PCs, só apareceram em meados da década de 80 e inicialmente foram utilizados como sistemas isolados; com o tempo, estes passaram a ser utilizados também como terminais de um computador central. (GOUVÊA, 1997).

No tocante à internet, o desenvolvimento desta pode ser resumido em duas importantes décadas: 1960 e 1970.

Nos anos 60, o Departamento de Defesa dos Estados Unidos elaborou um sistema de comunicação com o uso de redes de computadores. Assim, observa-se que, originalmente, a internet tinha como objetivo ser uma rede de comunicação à prova de impactos causados por bombas nucleares contra os Estados Unidos da América, em meados da Guerra Fria (1957), depois de a União Soviética lançar seu satélite espacial.

Nesse contexto, Rosa (2005, p. 31) explica que “a intenção era difundi-la de tal forma que, se os EUA viessem a sofrer bombardeios, tal rede permaneceria ativa, pois não existiria um sistema central e as informações poderiam trafegar por caminhos alternativos, até chegarem ao seu destinatário”.

Em 1970, houve uma expansão desse sistema de comunicação; a internet incorporou as universidades, a fim de ser utilizada para meios acadêmicos e propagação da liberdade de expressão, sendo relutada com força pelos países que adotavam os regimes chamados totalitários.

Com a popularização da Arpanet (*Advanced Research Projects Agency*), nome colocado para a rede de comunicações militares, foram criados o correio eletrônico, um fenômeno mundial, e a especificação do protocolo para transferência de arquivos, o FTP (*File Transfer Protocol*), outra aplicação fundamental na internet. (ROSA, 2005, p. 32).

Na década de 1990, a internet deixa de ser restrita aos meios militares e científicos e passa a ser uma Rede de comunicação e transferência de dados mundial. Junto com a internet, o avanço tecnológico se evidencia, tornando o ambiente computacional disperso, tanto geográfica quanto organizacionalmente, dando à comunicação de dados um papel relevante. A comunicação, juntamente com a rede e o armazenamento de dados, começam a ser disponíveis agora em dispositivos móveis, como os celulares, *tablets* e *smartphones* desta geração.

2.2 SEGURANÇA DA INFORMAÇÃO

Inicialmente, torna-se necessário explicar o que vem a ser informação. Derivada do latim *informare,* que significa "dar forma", esta palavra traduz todo o conteúdo trocado com o mundo exterior ao ajustar-se a ele. Para o computador, todo dado é informação, a qual é expressa por meio de uma codificação digital. (SILVA, 2003, p.27).

Na era da informação, a importância da segurança dos dados é uma característica essencial para os sistemas de informação. Isso porque, com o tempo, a necessidade de proteger dados pessoais e sigilosos se tornou evidente, e então surgiram métodos de proteção contra cópias ilegais, fraudes, invasão e furto de dados, principalmente no âmbito empresarial.

2.2.1 Conceito de Segurança da Informação

Nos termos do Código de Prática para a Gestão da Segurança da Informação: "é a proteção da informação contra vários tipos de ameaças para garantir a continuidade do negócio, minimizar riscos, maximizar o retorno sobre os investimentos e as oportunidades de negócios". (ISO 27002).

Batista (2006, p. 169) entende que "a segurança é imposta para minimizar os prejuízos da organização por paralisações não esperadas, garantir a qualidade dos dados inseridos e das informações geradas, e para assegurar que esses dados não sejam roubados (sic) ou alterados sem autorização".

Interessante ressaltar que não só no âmbito empresarial se vê a necessidade de proteção de informação. Isso porque as pessoas começaram a utilizar muitos dispositivos para armazenar informações pessoais, tais como fotos, arquivos, senhas, dentre outros, procurando agilizar o compartilhamento e acesso destes conteúdos, o que acabou propiciando também o cometimento de vários atos ilícitos.

Neste sentido, oportuno mencionar os dizeres de Corrêa (2000, p. 10):

> Da mesma forma que uma pessoa dirigindo um veículo pode sofrer um acidente ou cometer algum ato ilícito, quando, por exemplo, atropela ou abalroa seu carro por não ter obedecido à sinalização, outra pessoa navegando pela Internet é perfeitamente vulnerável à ação de *hackers*, vírus de computadores e fraudadores, podendo, até, cometer atos ilícitos, quando desrespeita os limites estabelecidos pelos sistemas de segurança de determinada empresa conectada à Rede, ou remete mensagens eletrônicas ameaçando outrem.

Como se vê, o sistema informático requer um método para a proteção de arquivos e dados a fim de garantir que as informações obtidas no sistema não sejam lidas ou alteradas. Para garantir esta proteção, foram desenvolvidos os chamados "mecanismos de segurança" que, quando corretamente utilizados pelos usuários, podem garantir a proteção de eventuais riscos advindos do uso de sistemas informáticos, sobretudo, quando o dispositivo informático estiver conectado à Rede.

Dito isto, passa-se a esclarecer acerca das vulnerabilidades dos sistemas informáticos, bem como expor as principais formas de ataques realizados contra estes sistemas. Por fim, serão apresentados mecanismos se segurança com o fim de prevenir ou detectar estes ataques à segurança dos sistemas.

2.2.2 Vulnerabilidade dos sistemas e uso indevido

Os sistemas de informação são compostos de inúmeros elementos que podem estar localizados em diversos lugares. Desta forma, cada sistema de informação fica vulnerável a perigos ou ameaças que podem ser criados.

Com relação ao conceito de vulnerabilidade, esta pode ser definida como:

> [...] condição que, quando explorada por um atacante, pode resultar em uma violação de segurança. Exemplos de vulnerabilidades são falhas no projeto, na implementação, ou na configuração de programas, serviços ou equipamentos de rede. Um ataque de exploração de vulnerabilidades ocorre quando um atacante, utilizando-se de uma vulnerabilidade, tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais, disparar ataques contra outros computadores ou tornar um serviço inacessível. (CARTILHA..., 2012, p. 18).

Complementarmente, Laudon e Laudon (2007, p. 210) explanam:

> Quando grandes quantidades de dados são armazenadas sob formato eletrônico, ficam vulneráveis a muito mais tipos de ameaças do que quando estão em formato manual. Sistemas de informação em diferentes localidades podem ser interconectados por meio de redes de telecomunicação. Logo, o potencial para acesso não autorizado, uso indevido ou fraude não fica limitado a um único lugar, mas pode ocorrer em qualquer ponto de acesso à rede.

A vulnerabilidade dos sistemas de informação é muito maior onde prevalece a computação em rede, uma vez que as redes públicas – incluindo a internet – estão mais sujeitas a perigos ou ameaças porque estão abertas a praticamente qualquer pessoa e, portanto, sujeitas às ações destas.

Percebe-se, portanto, que os sistemas estão sujeitos à vulnerabilidades, principalmente quando estes estiverem conectados à Rede. Logo, infere-se que, quanto mais *online* as pessoas estiverem, maiores serão os riscos de segurança.

2.2.3 Meios de violação da informação em rede digital

São muitos os mecanismos de ataques utilizados na internet. A intrusão é a forma mais conhecida, principalmente pelos *hackers.* Tal técnica consiste em utilizar o computador de outra pessoa como se fosse seu legítimo usuário. Vai desde a engenharia social até o uso de avançados recursos tecnológicos.

No tocante aos meios de violação de rede, os mais comuns e utilizados são os programas de *software* mal-intencionados, denominados de *malwares* (códigos maliciosos), os quais, uma vez instalados, permitem o acesso aos dados armazenados no computador.

Dentre as principais razões que levam um atacante a criar e propagar *malwares* destacam-se a obtenção de vantagens financeiras, a coleta de informações pessoais, o desejo de autopromoção ou, ainda, o vandalismo. Anota-se ainda que os códigos maliciosos são usados muitas vezes como intermédio para a prática de golpes. (CARTILHA..., 2012, p. 24).

Estes programas incluem uma variedade de ameaças, tais como *spywares*, cavalo de Tróia (*trojan horse*), vírus de computador e *phishing scam.* Agora cabe conhecer, ainda que de modo sucinto, cada um desses meios de violação.

2.2.3.1 Spyware

De forma sucinta Rosa (2005, p. 70) explica que o *spyware* é um "programa que monitora hábitos no computador, como padrões de navegação na *Web*, e transmite a informação a terceiros, às vezes sem a explícita autorização ou o consentimento do usuário".

O *spyware* apresenta anúncios indesejados e age como uma espécie de ladrão cibernético, sendo uma das maiores reclamações dos usuários da Rede. Isso porque um usuário pode facilmente instalar – sem permissão – o *spyware*, clicando – mesmo sem intenção – em propagandas, acessando sítios não seguros e abrindo *links* alternativos recebidos na caixa de *e-mail*.

Neste contexto, Laudon e Laudon (2007, p. 214) expõem que "muitos usuários consideram esses *spywares* incômodos, e alguns condenam seu uso, alegando que eles infringem a privacidade dos usuários de computador".

A problemática maior está na ação dos chamados *key loggers* (registradores de teclas), que são *spywares* que registram, literalmente, cada tecla pressionada pelo usuário de um computador a fim de obter acesso a contas de *e-mail* ou, ainda, coletar informações pessoais como números de cartão de crédito e senhas. (LAUDON; LAUDON, 2007).

Desta forma, tudo o que for utilizado, todas as informações digitadas, todas as senhas, poderão ser visualizadas através do *spyware* instalado, passando as informações para o criminoso responsável por este *software* malicioso.

2.2.3.2 Cavalo de Tróia (*Trojan Horse*)

Geralmente com uma aparência benéfica e que parece ter uma função útil, o cavalo de Tróia (*trojan horse*)[1] é um programa malicioso camuflado que inclui recursos escondidos a fim de danificar arquivos.

Rosa (2005, p. 69) acrescenta que esta espécie de programa "pode objetivar também a alteração de dados, cópia de arquivos com finalidade de obter ganhos monetários".

Através deste *software* (programa) malicioso, os sistemas são facilmente burlados tornando-se vulneráveis, uma vez que induz os usuários a utilizarem o programa com os tais recursos potencialmente maldosos.

[1] O "Cavalo de Tróia", segundo a mitologia grega, foi uma grande estátua, utilizada como instrumento de guerra pelos gregos para obter acesso a cidade de Tróia. A estátua do cavalo foi recheada com soldados que, durante a noite, abriram os portões da cidade possibilitando a entrada dos gregos e a dominação de Tróia. (CARTILHA…,2012, p. 28).

Esta espécie de programa pode também ser instalado por atacantes que, após invadirem um dispositivo informático, alteram programas já existentes neste para que, além de continuar a desempenhar as funções originais, também execute ações maliciosas. (CARTILHA..., 2012, p. 28).

Laudon e Laudon (2007, p. 213) salientam que "o cavalo de Tróia em si não é um vírus, porque não se replica, mas é muitas vezes uma porta para que vírus ou outros códigos mal-intencionados entrem no sistema de computador".

Usuários sem conhecimentos básicos de segurança facilmente são enganados por estes programas por sua aparência até então confiável e útil, achando ser um programa de boa execução, o qual instala, sem a permissão destes, um *software* capaz de desestabilizar o sistema e abrir brechas (vulnerabilidades) para que outros *malwares* possam se instalar.

Trata-se de um dos métodos mais utilizados atualmente para a invasão através da internet.

2.2.3.3 Vírus de computador

Os vírus geralmente danificam programas de tipo executável por serem códigos de computação que corrompem o sistema podendo, em várias ocasiões, gerar a necessidade de formatação do dispositivo informático, onde todo o sistema operacional é reinstalado, perdendo arquivos salvos.

Nas palavras de Batista (2006, p. 176):

> Os vírus de computador são programas "inteligentes" com autonomia para se autocopiar para dispositivos de intercâmbio de dados, como discos flexíveis e discos rígidos. O objetivo inicial dos programas de vírus é causar algum prejuízo para usuários e organizações, ou até mesmo como forma de prevenção de pirataria de *software.*

Rosa (2005, p. 69) coaduna dizendo que "o vírus é um segmento de programa de computação capaz de mudar a estrutura do *software* do sistema e destruir ou alterar dados ou programas ou outras ações nocivas, com ou sem o conhecimento do operador".

Em empresas, o problema aumenta ao danificar programas essenciais e pagos, os quais não possuem garantia, levando a empresa a comprar o pacote de programas por mais de uma vez. Dependendo do vírus, poderá haver a danificação até mesmo do mecanismo de segurança, deixando todo o sistema vulnerável.

O vírus está sempre oculto, tanto em sítios, programas ou *e-mails* e, assim como um vírus real, espalha-se pelo corpo até contaminá-lo por completo. O vírus virtual pode danificar todos os arquivos salvos, bem como conteúdos importantes e, dependendo do tipo de vírus, ainda danifica os *hardwares* e as peças responsáveis por memória, processamento e resfriamento do dispositivo informático alvo.

2.2.3.4 Phishing scam

Uma prática cada vez mais popular é a denominada *phishing scam*, que pode ser tanto a criação de sítios falsos como *e-mails* enviados que apresentam "aparentemente" serem enviados de sítios famosos, muito parecidos com o sítio original, a fim de pedir aos usuários dados pessoais confidenciais.

As mensagens de *e-mail* instruem o usuário a atualizar ou confirmar cadastros, fornecendo números confidenciais, tais como senhas de cartão de crédito, informações bancárias e outras informações; os dados são enviados automaticamente aos criminosos, como senhas e contas de bancos. (LAUDON; LAUDON, 2007).

Nogueira (2008, p. 42) conclui dizendo que "o pior de tudo, é que as pessoas acabam que por curiosidade, ingenuidade ou desinformação, acessando o link, fazendo com que abra o e-mail e seja instalado um programa para lhe furtar dados, senhas, entre outras coisas".

Portanto, o *phishing* pode ser traduzido como um meio de violação que engana os usuários, os quais possibilitam o acesso deste através de seu consentimento indireto.

2.2.4 Mecanismos de segurança

Como já demonstrado nos tópicos anteriores, os sistemas estão sujeitos a vulnerabilidades e, portanto, necessitam de mecanismos que devem ser utilizados com o fim de detectar ou prever um ataque à segurança dos sistemas.

A seguir, serão apresentadas as principais medidas de segurança utilizadas atualmente com o fim de prevenção aos chamados ataques contra sistemas informáticos.

2.2.4.1 Criptografia

A Criptografia é um recurso para proporcionar segurança de dados contra acessos indevidos através da codificação de dados em cifras e códigos, necessitando de uma chave adequada para a decodificação, possuída exclusivamente pelo titular que tem livre acesso a estes dados e informações.

Um exemplo usual de criptografia é a assinatura digital, uma espécie de código para verificar a integridade de um texto ou mensagem. Este mecanismo também pode ser utilizado para verificar se o remetente de uma mensagem é mesmo quem diz ser.

De forma sucinta, exemplifica Corrêa (2000, p.77):

> A criptografia seria uma "mascara" colocada sob determinado arquivo, tornando-o irreconhecível para aqueles que lhe "olhassem na rua", ou seja, enquanto estivesse trafegando na rede. Essa mascara seria algo lógico, relacionado a fórmulas matemáticas, e só alguém que possuísse a formula matemática certa poderia desmascará-la e, assim, lê-la.

Há basicamente duas modalidades de criptografia: a simétrica e a assimétrica. Aquela utiliza apenas uma chave de acesso para decodificar os dados, em que tanto o remetente quanto o destinatário utilizam a mesma, garantindo, assim, o sigilo das informações. Esta possui duas chaves distintas, uma para cada operação, protegendo também sua autenticidade.

Apesar de mais segura, a modalidade assimétrica é a menos utilizada.

2.2.4.2 Esteganografia

De forma sucinta, pode-se traduzir como uma técnica que possibilita a ocultação de um documento eletrônico, intercalando-o com os dados de outro arquivo eletrônico, de maneira codificada; logo, na ausência da chave esteganográfica, torna-se impossível decifrar ou identificar o arquivo camuflado.

2.2.4.3 Firewall

No sentido literal da palavra, *firewall* traduz-se como muralha de fogo; é um mecanismo que atua como defesa de um computador ou de uma rede, controlando o acesso ao sistema por meio de regras e filtragem de dados.

Também pode ser definido como um sistema, ou grupo de sistemas, que implanta uma política de controle de acesso entre duas redes. É normalmente utilizado como uma espécie de barreira entre a internet, ou outras redes internas. (TURBAN; McLEAN; WETHERBE, 2004).

Sendo assim, a barreira criada pelo *firewall* fornece informações de cada usuário a usar o dispositivo, não permitindo que usuários não autorizados trafeguem na rede local.

De forma objetiva, Laudon e Laudon (2007, p. 226) explicam que:

> O firewall age como um porteiro que examina as credenciais de cada usuário antes que ele possa acessar a rede. O firewall identifica nomes, endereços IP, aplicativos e outras características do trafego de entrada. Em seguida, compara essas informações com as regras de acesso que foram programadas no sistema pelo administrador da rede.

Muitas empresas utilizam internamente o *firewall* devido ao grande número de usuários conectados à rede interna, promovendo, assim, segurança no servidor local. Geralmente é utilizado a fim de que a empresa possa instalar uma política de segurança ao fluxo de tráfego entre as redes.

2.2.4.4 Antivírus

É visível a necessidade de se fazer varreduras periódicas no sistema, pois muitos *malwares*, programas e arquivos maliciosos conseguem ultrapassar os mecanismos de segurança que, em tese, deveriam evitar a instalação destes corpos estranhos.

Por tal motivo, alguns programas são específicos para esta varredura e remoção dos *malwares*. Estes programas são chamados de antivírus que, segundo Laudon e Laudon (2007, p. 229), "[...] é projetado para verificar sistemas de informação e *drivers*, a fim de detectar a presença de vírus de computador".

Logo, o antivírus é responsável por fazer varreduras, identificar e ainda bloquear qualquer ameaça no sistema informático.

2.3 CRIMES INFORMÁTICOS

É incontestável que o crescimento exponencial da internet juntamente com a popularização dos computadores e demais dispositivos informáticos trouxeram benefícios, pois estreitou a distância entre as pessoas, colocando-as em contato de forma simples e rápida.

No entanto, da mesma forma que o crescimento tecnológico trouxe avanços significativos para a sociedade em geral, acabou também se convertendo num terreno novo e convidativo para a prática de crimes e fraudes.[2]

Importante destacar que as maiorias destes delitos acabam sendo cometidos por ausência de conhecimento básico dos usuários-vítimas. Isso porque muitos destes não detêm conhecimento necessário para se protegerem das intrusões, tornando-se, assim, vítimas fáceis.

Os métodos utilizados pelos criminosos visam explorar a vulnerabilidade dos sistemas e dispositivos usados. Assim, uma vez detectada a vulnerabilidade, o crime informático é efetuado.

Dito isso, passa-se a uma breve análise dos denominados crimes informáticos, bem como de que maneira eles são cometidos e, ainda, quem são os sujeitos desta espécie de delito.

2.3.1 Nomenclatura

Inicialmente, cumpre mencionar que a questão da nomenclatura para crimes dessa natureza não se encontra padronizada no Brasil.

Entre as expressões mais comuns – algumas usadas de forma equivocada –, destacam-se as seguintes: crimes de informática, crimes tecnológicos, crimes virtuais, crimes cibernéticos, crimes de computação, crimes por meio de informática, infocrimes, delitos informáticos, criminalidade mediante computador, crimes digitais, dentre outros.

Com relação a estes diversos termos utilizados, Silva (2003, p. 54-55) observa:

> Impera a falta de unanimidade ao se buscar nominar as ações lesivas a bens jurídicos em que se tenha o sistema informático presente, quer na ação do sujeito, quer como objeto dela. Deve-se, pois, cuidar ao usar a expressão *crime* ou *delito*, uma vez que, tecnicamente, referem-se à ação ou omissão, típica, antijurídica e culpável e, assim sendo, quando se reconhece a necessidade de tipificação para algumas condutas, conseqüentemente, o seu uso é inadequado.

Contudo, será utilizado o termo “crimes informáticos” no presente trabalho, por se tratar de expressão que traduz não somente o computador em si ou o meio informático, mas abrange todos os equipamentos informáticos que de alguma forma possam servir como meio de transmissão de dados e, ainda, refere-se a toda tecnologia que possa ser por eles utilizada.

Feita tal consideração, passa-se a analisar o conceito de crime informático.

---

[2] O crime informático já é a terceira modalidade de crime que mais causa prejuízo ao mundo depois do narcotráfico e da falsificação de marcas e de propriedade industrial. (SCIARRETTA, 2014).

2.3.2 Conceito

Oportuno, neste momento, conceituar o que venha a ser crime informático, e para isto utilizar-se-á a melhor doutrina sobre o tema.

Rosa (2006, p. 58) o define como "[...] conduta típica, ilícita e culpável, praticada sempre com a utilização de dispositivos de sistemas de processamento ou comunicação de dados, da qual poderá ou não suceder a obtenção de uma vantagem indevida e ilícita".

Nos dizeres de Silva (2003, p. 58), "trata-se de ação ou omissão, típica, antijurídica e culpável, produzida por meio de atividades que envolvam dispositivos que integram o sistema informático, lembrando sempre que a referência se faz aos casos em que há relação típica".

Para Castro (2003, p. 9), crime informático pode ser entendido como:

> [...] aquele praticado contra o sistema de informática ou através deste, compreendendo os crimes praticados contra o computador e seus acessórios e os perpetrados através do computador. Inclui-se neste conceito os delitos praticados através da Internet, pois pressuposto para acessar a rede é a utilização de um computador.

E ainda, no conceito de Corrêa (2000, p. 43), "[...] seriam todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar [...]".

Como se vê, não há uma conceituação uniforme para os denominados crimes informáticos. Nesse viés Silva (2003, p. 57) conclui: "[...] ora se observa o sistema informático como elemento indissociável da conduta praticada pelo agente, ora este papel é assumido apenas pelo computador, ora se citam ambos, como elementos integrantes do conceito".

Denota-se, contudo, que qualquer tentativa de conceituação para 'crime informático', apresentará falhas. Isso porque dificilmente é possível se elaborar uma definição clara e precisa que abranja todos os aspectos do crime.

Ademais, tendo em vista que o crime informático por vezes envolverá várias outras espécies de crime, não se deve adotar uma expressão estática e formal, o que poderia acarretar mais dúvidas quanto à sua definição. (ALBUQUERQUE, 2006).

2.3.2 Classificação

Encontra-se na doutrina algumas classificações para os chamados crimes informáticos. Dentre elas, a doutrina de Albuquerque (2006, p. 40-41) aponta que:

> [...] São, basicamente, duas as espécies de crimes informáticos, os crimes informáticos comuns e os crimes informáticos específicos. Nos crimes informáticos comuns, a informática é utilizada como meio para a prática de condutas que já são consideradas crime pelo direito penal vigente. A conduta ilícita já é objeto de punição. A situação não é a mesma com os crimes informáticos específicos, em que se praticam condutas contra bens jurídicos que ainda não são objeto de tutela penal.

Considerando as diversas classificações existentes, todas análogas, adota-se, no presente trabalho, a classificação dos crimes informáticos em próprios ou puros e impróprios ou impuros.

Os crimes informáticos impróprios/impuros – popularmente conhecidos como ‘crimes com o computador’ –, são aqueles que abarcam condutas em que o sistema informático figura apenas como o meio, o instrumento para a realização do crime. Um exemplo comum deste tipo de crime é o crime contra a honra, que independente do meio, poderá ocorrer através de outros meios de execução, e não necessariamente o meio informático.

No que concerne aos crimes informáticos próprios/puros – popularmente conhecidos como ‘crimes contra o computador’ –, estes, por sua vez, abrangem condutas que ferem bens jurídicos inerentes ao próprio sistema informático, atingindo os dados, informações ou estruturas a ele ligados; logo, pode-se dizer que fere a intimidade contida dentro do próprio meio de computador. Um exemplo clássico deste crime seria a invasão de conta de *e-mail* ou de rede social de um indivíduo ou, ainda a invasão de dados armazenados no próprio dispositivo informático.

.

2.3.3 Sujeitos

2.3.3.1 Sujeito ativo

Em um dos primeiros livros editados no Brasil sobre crimes informáticos, Gouvêa (1997, p. 60) aduz:

> Pode-se afirmar que, na década de 70, a maioria dos crimes era cometida por programadores, já que naquela época a dificuldade no uso de computadores exigia um vasto conhecimento técnico para a prática destes delitos. Como cada vez mais pessoas fazem uso das máquinas, houve uma disseminação destes crimes. Na década de 80, foram detectadas as primeiras fraudes bancárias. Os funcionários dos bancos têm acesso a dados relativos à movimentação de inúmeras contas correntes, aplicações, etc. Hoje em dia, com a massificação dos computadores e das redes, qualquer pessoa pode praticar delitos através da informática.

Portanto, em regra, o criminoso informático é um operador de computadores e sistemas informáticos, porém, não se pode generalizar. Conforme será verificado no decorrer da presente monografia, a modalidade de crime de invasão de dispositivo informático (CP, art. 154-A), por exemplo, pode ser praticada por qualquer indivíduo que saiba manusear um dispositivo informático. (BRASIL, 1940).

Os criminosos informáticos podem ser classificados em duas categorias: os profissionais e amadores. Os primeiros dizem respeito aos indivíduos com vasta experiência em invasão de sistemas, responsáveis em praticar crimes que envolvem grandes prejuízos econômicos para as vítimas. Quanto à segunda categoria, compreendem-se os jovens gênios de informática, os quais aprenderam técnicas importantes, tais como a violação de códigos de segurança. (ALBUQUERQUE, 2006).

A seguir, será explanado sucintamente as espécies e características dos sujeitos mais comuns, praticantes destes delitos.

2.3.3.1.1 Hackers

Embora muito confundido como invasores de sistemas, os *hackers* são profissionais da área de informática, os quais possuem conhecimentos necessários para a possibilidade de manipular e alterar o sistema de informação.

Geralmente, os *hackers* são contratados por empresas para desenvolverem mecanismos de seguranças, a fim de proporcionar ao sistema e banco de dados, proteção contra violações na rede. Estes indivíduos procuram vulnerabilidades e fragilidades nas proteções de segurança empregadas pelos sítios e sistemas de computador.

Sobre a intenção destes sujeitos, Corrêa (2000, p. 57) afirma:

> Um *hacker* pode querer acessar determinado sistema por um grande número de razões. Pode ele simplesmente querer obter uma informação particular dentro daquele sistema, somente lendo-a, mas pode também adentrar um sistema para fins ilícitos, como extorquir alguém, ter acesso a mensagens particulares, furtar informações de grande valor pecuniário, destruir dados, disseminar vírus e muito mais, querendo, muitas vezes, obter lucros.

Observa-se, portanto, que o que pode caracterizar um *hacker* como ameaça é sua intenção e acesso não autorizado a sistemas e dispositivos para cometer crimes, fraudes eletrônicas e bancárias, bem como furtos de dados. Quando isto ocorre, este passa a ser denominado de *cracker*, conforme se explicará adiante.

2.3.3.1.2 Crackers

Conhecido no mundo *hacking* como sendo o *hacker* mal intencionado, os *crackers* são *hackers* profissionais com conhecimento suficiente para a manipulação de sistemas, que violam redes de segurança e sistemas a fim de obterem informações e dados, conteúdos privados de empresas e pessoas, para depois comercializar tais informações ou expor de alguma maneira estas mesmas.

Neste sentido, corrobora Nogueira, (2008, p. 61):

> Este indivíduo usa a internet para cometer crimes, fraudes bancárias e eletrônicas, furto de dados, golpes e grandes estragos. São verdadeiras quadrilhas de jovens que não se contentam apenas em invadir um sistema, usam sua inteligência e domínio da informática pra causar prejuízos de milhares de reais, tanto contra pessoas físicas, como jurídicas, órgãos públicos, etc.

Logo, pode-se afirmar que nem todos os *hackers* são criminosos virtuais, apenas parte deles, os quais possuem, inclusive, denominação própria, qual seja: *crackers.*

2.3.3.1.3 Phreakers

No meio de comunicação através da telefonia fixa e móvel existem invasores que visam obter vantagens e cometer fraudes.

Conhecidos como *phreakers,* estes sujeitos são especialistas em telefonia e, nos dizeres de Rosa (2006, p. 61), "atuam na obtenção de ligações telefônicas gratuitas e instalação de escutas, facilitando o ataque a sistemas a partir de acesso exterior, tornando-se invisíveis ao rastreamento ou colocando a responsabilidade em terceiros".

Neste contexto, Nogueira (2008, p. 61) conclui*:* "[...] este indivíduo é o terror das companhias telefônicas, pois são especialistas em burlar sistemas de telefonia, fixa ou móvel, os prejuízos são enormes e incalculáveis".

2.3.3.1.4 Spammers

Os *spammers* são pessoas ou empresas que enviam e-mails indesejados, usando um método abusivo de exagero para todas as caixas de *e-mails* possíveis.

Muitas vezes os *spams* – nome dado para estes *e-mails* indesejados e não solicitados –, podem conter vírus, além de superlotar as caixas de entrada do correio eletrônico. A título de informação, um levantamento feito mostrou que cerca de 60% dos *e-mails* recebidos pelos usuários atualmente são *spams.* (NOGUEIRA, 2008).

2.3.3.1.5 Pichadores virtuais

Os pichadores virtuais geralmente ganham notoriedade, pois invadem sistemas de segurança e deixam uma marca, a fim de demonstrar que foram eles quem invadiram.

Neste sentido, Nogueira (2008) afirma que estes criminosos costumam violar sítios (geralmente do poder público), como do FBI, Pentágono, Supremo Tribunal Federal. Por vezes, estas invasões ocorrem como forma de manifesto político ou religioso que, normalmente não causam danos patrimoniais.

Os pichadores virtuais geralmente são formados por grupos de *hackers* que almejam um desafio, para ao fim, demonstrar que "superaram" este desafio.

2.3.3.2 Sujeito passivo

É o sujeito titular do bem jurídico lesado ou ameaçado de lesão. Dependendo da natureza do crime, o sujeito passivo poderá ser a pessoa física ou jurídica, o Estado, a coletividade ou, ainda, a comunidade internacional. (SILVA, 2003, p. 82).

É importante mencionar, entretanto, que o principal alvo dos agentes criminosos são as instituições financeiras e empresas telefônicas. Diante disto, uma curiosidade está no fato de estas vítimas optarem pelo silêncio quanto à lesão sofrida, ao terem de arcar com os prejuízos advindos desta.

Nas palavras de Rosa (2006, p. 63), estas grandes empresas têm "[...] medo do desprestígio e da consequente perda da credibilidade que, talvez, isso possa causar, pois poderá dar a impressão de que esta ou aquela instituição não possui sistemas de segurança eficazes".

No entanto, é válido dizer que hoje em dia não é cabível restringir a tutela para determinados sujeitos. A verdade é que com a massificação do acesso à internet, somada ao crescente uso dos computadores e demais dispositivos informáticos, qualquer pessoa pode hoje praticar delitos desta natureza, bem como qualquer indivíduo pode se tornar vítima do mesmo.

3 DIREITO PENAL E INFORMÁTICA: QUESTÕES RELATIVAS À TUTELA JURÍDICO-PENAL DOS CRIMES INFORMÁTICOS

3.1 O TRATAMENTO DOS CRIMES INFORMÁTICOS NO BRASIL E A NECESSIDADE DE TIPIFICAÇÃO PARA CONDUTAS NÃO ABARCADAS PELA LEGISLAÇÃO PENAL VIGENTE

Conforme exposto nas linhas iniciais do presente trabalho, o avanço tecnológico propiciou o surgimento de novas práticas delituosas, considerando que o computador, em especial a internet, tornou-se um meio propenso e eficaz para a realização de tais delitos.

Assim, em virtude do anonimato que a internet proporciona, aliado à ausência de legislação brasileira específica ao assunto, tal modalidade de delito aumentou consideravelmente, de modo a obrigar a população e as autoridades a buscarem métodos de prevenção contra os criminosos. (CARLI, 2006).

Albuquerque (2006, p. 1) corrobora tal entendimento afirmando que: "Redes de computadores e sistemas de telecomunicação têm atraído a atenção de infratores, que podem aproveitar-se de lacunas existentes no sistema jurídico para gozar da impunidade".

Dito isto, oportuno destacar que é maciço o entendimento de que o Direito Penal deve ser invocado como *ultima ratio*, ou seja, este deve ser aplicado somente nas hipóteses em que há efetiva lesão a um bem jurídico relevante; deve ser visto como um instrumento a ser utilizado pelo Estado, nas situações em que a aplicação de outro tipo de Direito tornou-se insuficiente ou ineficiente.

Logo, considerando tal entendimento, e atrelando-o com a realidade fática acerca do aumento das praticas delituosas que imperam sobre o meio informático, tornou-se relevante e indispensável o combate destes crimes através da legislação penal. Ora, o Direito Penal não pode ficar inerte a tal situação, pois isso fortaleceria a ideia de que o meio informático – principalmente a internet – é um território isento de lei, ficando à margem da tutela jurisdicional do Estado.

Este é o entendimento de Pinheiro (2009, p. 230-231):

> O maior estímulo aos crimes virtuais é dado pela crença de que o meio digital é um ambiente marginal, um submundo em que a ilegalidade impera. Essa postura existe porque a sociedade não sente que o meio é suficientemente vigiado, que os seus crimes são adequadamente punidos. O conjunto norma-sanção é tão necessário no mundo digital quanto no real.

Nos dizeres de Corrêa (2000, p. 58), "a lei é, e sempre será, essencial para a prevenção e punição dos crimes, sejam estes dentro do mundo material ou digital".

No entanto, é cediço que no Brasil não se pode enquadrar como crime, conduta que não tenha previsão legal, pois isso feriria o Princípio da Legalidade (reserva legal)[3] previsto no artigo 5º, inciso XXXIX da Constituição Federal, que estabelece: "Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal". (BRASIL, 1988).

Mencionado princípio encontra-se ratificado no artigo 1º do Código Penal, com redação que pouco difere daquela contida na Lei Maior, a saber: "Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal". (BRASIL, 1940).

Em respeito a tal princípio, torna-se inadmissível em matéria de Direito Penal, o emprego de analogias no tocante às normas incriminadoras, em especial, a denominada analogia maléfica (*in malam partem),* qual seja, aquela utilizada em prejuízo do agente.

A respeito disso, Capez (2010, p. 55) reforça o entendimento exemplificando que:

> A aplicação da analogia em norma penal incriminadora fere o princípio da reserva legal, uma vez que um fato não definido em lei como crime estaria sendo considerado como tal. Imagine considerar típico o furto de uso (subtração de coisa alheia móvel para uso), por força da aplicação analógica do art. 155 do Código Penal (subtrair coisa alheia móvel com ânimo de assenhoreamento definitivo). Neste caso, um fato não considerado criminoso pela lei passaria a sê-lo, em evidente afronta ao princípio constitucional do art. 5º, XXXIX (reserva legal).

Feito tais ponderações, conclui-se que num regime democrático de direito toda conduta proibida deve estar legalmente prevista.

Em relação aos crimes informáticos, constata-se que o Poder Judiciário, os membros do Ministério Público, bem como as autoridades policiais vêm utilizando tipos penais já existentes no Código Penal e Leis Penais Especiais para enquadrar os delitos cometidos pelo meio virtual.

A doutrina tem sido uníssona ao afirmar que o crime informático é, em princípio, um crime de meio, isto é, utiliza-se de um meio virtual para o seu cometimento. Não é um crime de fim, por natureza, cuja modalidade só ocorra em ambiente virtual. (PINHEIRO, 2009).

---

[3] No tocante aos princípios da legalidade e reserva legal, há três entendimentos diversos na doutrina no que diz respeito às suas definições. O primeiro entendimento é de que os dois princípios seriam sinônimos. De outro lado, há o entendimento de que o princípio da legalidade no Direito Penal seria a junção dos princípios da reserva legal e da anterioridade (corrente majoritária). Por último, há o entendimento de que os dois princípios não se confundem, podendo definí-los de maneira independente. Assim, a legalidade refere-se a lei em sentido amplo, ou seja, todas as espécies normativas previstas na Constituição Federal. O princípio da reserva legal, por sua vez, determina que somente a lei em sentido estrito (lei ordinária ou complementar) pode criar regras no Direito Penal.

Assim, alguns doutrinadores advogam a tese de que a maioria destes crimes poderia muito bem ser abarcada pela legislação penal vigente, uma vez que se encaixam às incriminações convencionais já tipificadas.

Em determinados casos, considerando o bem jurídico tutelado, o computador atua como um mero instrumento para a prática delitiva; o que modifica é apenas o meio, a sua instrumentalização, não tendo que se falar, portanto, na criação de novos tipos penais nestes casos. É o que ocorre, por exemplo, com os crimes contra a honra, fraude, furto, estelionato, pornografia infanto-juvenil, terrorismo, entre outros, quando praticados pelo meio informático.

Este também tem sido o posicionamento dos Tribunais Superiores, dentre eles o Supremo Tribunal Federal, conforme se verifica na decisão do Habeas Corpus nº 76689/PB, *in verbis:*

> 'Crime de Computador': publicação de cena de sexo infanto-juvenil (E.C.A., art. 241), mediante inserção em rede BBS/Internet de computadores, atribuída a menores: tipicidade: prova pericial necessária à demonstração da autoria: HC deferido em parte. 1. O tipo cogitado –na modalidade de "publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente" – ao contrário do que sucede, por exemplo, aos da Lei de Imprensa, no tocante ao processo da publicação incriminada é uma norma aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador. 2. Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta criminada, **o meio técnico empregado para realizá-la pode até ser invenção posterior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo.** 3. Se a solução da controvérsia de fato sobre a autoria da inserção incriminada pende de informações técnicas de telemática que ainda pairam acima de conhecimento do homem comum, impõe-se a realização de prova pericial. (BRASIL, 1998. Supremo Tribunal Federal. 1ª Turma. HC 76689, TJPB / Rel: Min. Sepúlveda Pertence. Data do julgamento: 22/09/1998. Data de publicação no DJe: 06/11/1998, grifo meu).

De fato, há pertinência neste entendimento, pois, ao punir estes indivíduos com base nos tipos penais já definidos na legislação em vigor, o Poder Judiciário não estaria violando o princípio da legalidade (ou da reserva legal).

Mas importante esclarecer que há determinadas condutas que, devido às suas peculiaridades, não encontram amparo na legislação, necessitando, assim, de tipificação própria. Nessa reflexão, Pinheiro (2009, p. 226) aduz que:

> A maioria dos crimes cometidos na rede ocorre também no mundo real. A Internet surge apenas como um facilitador, principalmente pelo anonimato que proporciona. Portanto, as questões quanto ao conceito de crime, delito, ato e efeito são as

> mesmas, quer sejam aplicadas para o Direito Penal ou para o Direito Penal Digital. As principais inovações jurídicas trazidas pelo âmbito digital se referem à territorialidade e à investigação probatória, bem como à necessidade de tipificação penal de algumas modalidades que, em razão de suas peculiaridades, merecem ter um tipo penal próprio.

Portanto, constata-se um vazio legiferante no que pertine a certas condutas praticadas ou não por meio da internet que envolvem tecnologia, dado, informação e sistema equivalente, tendo em vista que determinadas situações não foram expressamente tuteladas pelo Código Penal e leis penais especiais brasileiras.

Grosso modo, pode-se dizer que a proliferação dos delitos informáticos ocorre paralelamente com o avanço dos sistemas de informática e dos recursos que estes instrumentos oferecem. O armazenamento de dados e informações pessoais e profissionais tais como contas bancárias, contas de *e-mails* e redes sociais, número de cartão de crédito e outras informações são conteúdos que despertam o interesse do agente criminoso.

Talvez por isso, houve uma necessidade de se buscar mecanismos de proteção no âmbito penal a fim de obter segurança e a garantia da privacidade que as pessoas devem gozar livremente. Segundo Cabette (2013), "[...] o fenômeno informático está a exigir regulamentação especial devido às suas características que divergem de tudo quanto sempre foi usual".

Tal quadro acabou por impulsionar a promulgação da Lei n. 12.737/2012, conhecida como "Lei Carolina Dieckmann", no intuito de suprir as lacunas até então existentes no ordenamento jurídico em face da prática de tais delitos. (BRASIL, 2012).

Entretanto, insta destacar que a lei suso mencionada foi fruto de fervorosos embates no cenário jurídico-político. Frisa-se que antes da edição dela, existiram outros projetos de lei objetivando a regulamentação dos crimes informáticos no Brasil, dos quais se destacam dois, por serem os mais importantes, conforme irá ser brevemente demonstrado adiante.

3.1.1 Propostas legislativas para a regulamentação brasileira acerca dos crimes informáticos

3.1.1.2 Projeto de lei nº 84/1999

Uma das propostas legislativas de maior repercussão social no tocante aos crimes informáticos foi, sem dúvida, o projeto de lei nº 84 (BRASIL, 1999).

Com origem na Câmara Federal, e de autoria do Deputado Luiz Piauhylino Monteiro, do Estado de Pernambuco, tal projeto propôs a criação de lei especial sobre crimes informáticos, incluindo penalidades. O projeto continha dezoito artigos, sendo que sete deles tipificavam crimes.

Nas palavras de Corrêa (2000, p. 85-86), "o autor do referido projeto procurou, à luz da natureza e do funcionamento dos computadores e suas redes, definir responsabilidades em relação à operação e ao seu uso, tipificando os 'crimes' relacionados com tais atividades e suas consequentes penalidades".

Anota-se, contudo, que o referido projeto de lei resultou em repercussão nacional a partir do momento em que o Deputado Eduardo Azeredo elaborou um substitutivo[4] ao texto aprovado pela Câmara em 2003. (HAJE, 2011).

Tal substitutivo desencadeou diversas críticas de internautas no tocante ao seu conteúdo, e por tal razão, o referido projeto de lei ficou popularmente conhecido como AI-5 Digital (menção ao Ato Institucional nº 5 do regime militar[5]), tendo em vista que seu texto suprimia a liberdade de expressão dos internautas e restringia o uso da Internet. Além disso, o substitutivo tipificaria como crime um simples *download* de arquivos[6].

3.1.1.2 Projeto de lei nº 2793/2011

Apresentado pelos deputados estaduais Paulo Teixeira e Manuela D'Ávila, este projeto de lei veio para solucionar o impasse do projeto de lei nº 84 (BRASIL, 1999), cuja redação, além de prolixa, caso fosse aprovada em sua integralidade, traria consequências prejudiciais para a sociedade, como, por exemplo, criminalizar o desbloqueio de aparelhos celulares. (MAZZARDO; GÖSSLING, 2013).

Ademais, os autores do projeto argumentaram que por conter menos disposições legais que o PL 84 (BRASIL, 1999), o PL 2793 (BRASIL, 2011) seria mais proveitoso para a sociedade, pois incentivaria a criação de tipos penais para crimes ainda não amparados na legislação penal até então vigente. (ROCHA, 2013).

---

[4] Espécie de emenda que altera a proposta em seu conjunto, substancial ou formalmente. Recebe ese nome porque substitui o projeto. O substitutivo é apresentado pelo relator e tem preferencia na votação, mas pode ser rejeitado em favor do projeto original.

[5] Considerado o mais severo golpe na democracia brasileira, o Ato institucional nº 5, de 1969 (AI-5 militar) instituiu a supressão dos direitos políticos de organização e expressão de idéias, agravando, assim, a repressão do regime militar.

[6] Art. 285-A. Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso.
Pena - reclusão, de 1 (um) a 3 (três) anos, e multa. (BRASIL, 1999).

Tal ideia encontra-se consubstanciada na própria justificativa da proposta parlamentar, a saber:

> A nosso ver, o PL 84/1999, em sua redação atual, traz propostas de criminalização demasiadamente abertas e desproporcionais, capazes de ensejar a tipificação criminal de condutas corriqueiras praticadas por grande parte da população na Internet. Ainda, fixa em um diploma penal matérias – como guarda e acesso de registros de conexão – que deveriam constar de uma regulamentação da Internet que fosse mais abrangente e mais atenta aos direitos e garantias do cidadão. (BRASIL, 2011).

No entanto, toda a problemática que circundava os projetos de lei em trâmite no Congresso só teve término com a repercussão nacional acerca do fato ocorrido com a atriz global Carolina Dieckmann, em maio de 2012, o que acabou por acelerar a aprovação do PL 2793 (BRASIL, 2011), culminando, assim, na publicação da Lei n. 12.737 (BRASIL, 2012), objeto do presente estudo.

3.2 DA LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012 – "LEI CAROLINA DIECKMANN"

Publicada no Diário Oficial da União em 03 de dezembro de 2012, e em vigor 120 (cento e vinte) dias após a sua publicação oficial, a Lei n. 12.737 "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". (BRASIL, 2012).

Apelidada de "Lei Carolina Dieckmann", ela deflagrou alterações no Código Penal (BRASIL, 1940). Acrescentou os artigos 154-A e 154-B, tipificando a conduta de "Invasão de dispositivo informático" e inseriu o § 1º ao artigo 266, tipificando como crime a conduta de interromper "serviço telemático ou de informação de utilidade pública". (BRASIL, 2012).

Por fim, inseriu o parágrafo único ao artigo 298 do mesmo Código (BRASIL, 1940), equiparando a falsificação ou alteração de cartão de crédito ou de débito ao crime de falsificação de documento particular (CP, art. 298, *caput*).

Passa-se a tecer, adiante, algumas considerações acerca do cenário que envolveu a promulgação da Lei "Carolina Dieckmann" (BRASIL, 2012) e, ainda, um breve estudo do crime de invasão de dispositivo informático (CP, arts. 154-A e 154-B), o qual será enfoque do presente trabalho monográfico.

3.2.1 O episódio midiático Carolina Dieckmann

Em maio de 2012, um episódio envolvendo a atriz Carolina Dieckmann (popularmente conhecida por seus papeis em telenovelas da Rede Globo) provocou intensa pressão social para a criminalização de condutas intimamente ligadas à chamada segurança informática, que há tanto tempo se discutia seja no meio acadêmico, seja no Poder Legislativo.

De acordo com os fatos noticiados pelos mais variados meios de comunicação na época, o computador da atriz teria sido invadido por *crackers* que, em razão de certas vulnerabilidades do sistema, obtiveram a senha de seu *e-mail* e "baixaram" fotos íntimas da atriz seminua e em posições em que expunha a sua intimidade. Todo o conteúdo foi indevidamente publicado na Rede mundial de computadores, inclusive, em sítios pornográficos. Além disso, a atriz sofreu tentativa de extorsão, por meio de telefonemas e *e-mails* para que as imagens não fossem divulgadas. Por fim, os infratores foram presos e, concomitantemente, foram apreendidos os computadores e demais instrumentos da prática delituosa. (ROCHA, 2012).

A verdade é que várias especulações foram feitas acerca do procedimento técnico adotado pelos infratores, a fim de obterem as fotografias íntimas da atriz. Inicialmente, acreditava-se que a suposta invasão e obtenção das fotos teriam ocorrido pelos técnicos da assistência autorizada, uma vez que a atriz teria levado o equipamento para manutenção. (BORGES; WENECK, 2012).

Tal hipótese foi rechaçada, uma vez que, de acordo com as investigações, um dos agentes criminosos teria invadido o *e-mail* da atriz, após enviar uma mensagem para ela, fingindo ser um representante do provedor de internet usado por ela. A mensagem continha um formulário, o qual foi preenchido pela atriz com seus dados pessoais, bem como a senha do *e-mail.* (GOMES, M., 2012).

Logo, uma vez fornecida a senha do *e-mail,* o criminoso teve acesso a todo o conteúdo presente no correio eletrônico da atriz, inclusive as fotos, que foram posteriormente divulgadas em meios eletrônicos e redes sociais.

3.2.2 A aceleração do processo legislativo e a aprovação da Lei nº 12.737/2012

O caso ocorrido com a atriz Carolina Dieckmann acabou servindo de estopim para a publicação da Lei n. 12.737 (BRASIL, 2012).

Isso porque, segundo Cabette (2013), o "[...] episódio acabou acelerando o andamento de projetos que já tramitavam com o fito de regulamentar essas práticas invasivas perpetradas em meios informáticos para modernização do Código Penal Brasileiro".

Atente-se que diferentemente do que foi exposto por meio de diversos veículos midiáticos, o episódio Carolina Dieckmann não motivou a lei, mas acabou por acelerá-la. Como já ressaltado, os projetos de lei já tramitavam no Congresso por mais de uma década com o intuito de sanar, ou ao menos amenizar, a problemática dos crimes informáticos no Brasil.

No tocante à sua publicação, Penido (2013) afirma que "[...] antes da Lei 12.737/2012, os especialistas da área de direito penal eletrônico afirmavam que 95% dos crimes ocorridos no meio informático já estavam previstos, havendo necessidade de se preencher essa lacuna de 5%".

Chega-se à conclusão, portanto, que a lei em comento surgiu com a finalidade de alcançar os denominados crimes informáticos próprios, objetivando proteger as informações ou bancos de dados dos computadores e demais dispositivos informáticos tais como celular, *pendrives*, *tablets* e *smartphones*, conectados ou não à Rede Mundial de Computadores.

No item seguinte, será feita uma breve análise da tipificação penal do crime de invasão de dispositivo informático, previsto nos artigos 154-A e 154-B, ambos acrescidos ao Código Penal (BRASIL, 1940), pois trata-se do delito de maior correlação com a temática do presente trabalho. (BRASIL, 1940).

3.2.3 Análise da tipificação penal do crime de Invasão de dispositivo informático (CP, arts. 154-A e 154-B)

Localizada à Seção IV ("Dos crimes contra a inviolabilidade dos segredos"), do Capítulo VI ("Dos crimes contra a liberdade individual"), do Título I ("Dos crimes contra a pessoa") do Código Penal Brasileiro (BRASIL, 1940), assim dispõe a norma penal incriminadora acrescida pela Lei n. 12.737 (BRASIL, 2012), *in verbis:*

> 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, governador 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. (BRASIL, 1940).

Por se tratar de uma lei recente e, portanto, ainda carente de publicações doutrinárias a respeito, far-se-á a análise do tipo penal acrescido ao Código Penal de 1940 (arts. 154-A e 154-B) com arrimo a artigos e estudos já publicados por alguns juristas e operadores de direito atuantes na área de direito penal e direito eletrônico.

3.2.3.1 Bem jurídico protegido

Observa-se que o bem jurídico protegido nesta espécie de crime é a privacidade, (gênero do qual são espécies a intimidade e a vida privada), sobretudo porque procura proteger dados e informações armazenadas em dispositivo informático.

Trata-se, portanto, de um direito fundamental protegido constitucionalmente, cujo amparo encontra-se no artigo 5º, inciso X da Constituição Federal, o qual dispõe que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito de indenização pelo dano material ou moral decorrente de sua violação". (BRASIL, 1988).

3.2.3.2 Sujeitos

3.2.3.2.1 Sujeito Ativo

O sujeito ativo pode ser qualquer pessoa, tendo em vista que o tipo penal não exige nenhuma qualidade especial do agente.

3.2.3.2.2 Sujeito Passivo

Em regra, o sujeito passivo é o titular do dispositivo, seja ele pessoa física ou jurídica.

No entanto, há outras hipóteses em que também se configura o sujeito passivo do crime, figurando no mesmo sentido, por exemplo, a pessoa que utiliza um computador de *lan house.*

Também seria o caso do sujeito que, apesar de não ser o proprietário do dispositivo informático, é quem efetivamente o utiliza para armazenar dados ou informações quem foram acessados indevidamente. É o caso, por exemplo, de um computador utilizado por várias pessoas de uma casa ou local de trabalho, onde cada uma delas possui um perfil e senha próprios. (ROCHA, 2012).

Por conseguinte, será considerado sujeito passivo do crime qualquer indivíduo que possa sofrer algum dano (material ou moral) ocasionado pela invasão, seja o proprietário ou possuidor do dispositivo informático, ou, ainda, terceiros prejudicados, em ocasiões em que a invasão atingir interesses de outros indivíduos.

3.2.3.3 Conduta típica

No tocante à conduta típica do agente, apesar de ainda não haver entendimento doutrinário ou jurisprudencial a fim de disciplinar a matéria, encontrou-se divergência entre os juristas que publicaram seus pareceres quanto ao tipo penal em questão.

O primeiro entendimento é no sentido de que o crime previsto no artigo 154-A do Código Penal (BRASIL, 1940) possui dois núcleos de conduta típica, representados pelos verbos invadir ou instalar. Neste sentido, o dispositivo informático da vítima poderia sofrer a invasão ou a instalação de vulnerabilidades. Ademais, o agente criminoso poderia incidir em

ambas as condutas, desde que num mesmo contexto, respondendo por crime único (tipo penal misto).[7]

De outro vértice, há a interpretação de que o referido tipo penal contém apenas uma conduta nuclear, representada pelo verbo invadir, com duas finalidades, quais sejam "obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo" ou "instalar vulnerabilidades para obter vantagem ilícita".[8]

Independente do entendimento adotado, importante observar que tal divergência existe porque o legislador não deixou claro na redação do tipo penal, se a parte final "ou instalar vulnerabilidades para obter vantagem ilícita" seria uma segunda conduta, ou outro especial fim de agir ou ainda se, a intenção foi deixar o verbo "instalar" no final da redação, possibilitando assim o enquadramento do agente nas duas condutas (invadir e instalar), ou apenas em uma (instalar vulnerabilidades).

No que diz respeito ao entendimento de possuir o tipo penal duas condutas (invadir ou instalar), acredita-se que os juristas que interpretam dessa forma levaram em consideração o fato de que uma invasão em ambiente informático pode ocorrer de várias formas: às vezes a instalação de um código malicioso (vulnerabilidade) serve como um meio de o agente invadir o sistema através da execução deste programa pelo usuário (muito comum através do método cavalo de Tróia); outras vezes o agente invade um dispositivo informático e, além da invasão, também instala uma vulnerabilidade a fim de monitorar as atividades de um sistema, como ocorre com os chamados *spywares.*

3.2.3.4 Elementares do tipo penal

3.2.3.4.1 Invadir

O verbo invadir, em regra, significa o ingresso, sem autorização, em determinado local.

Neste contexto, interessante a ponderação feita por Siena (2013), a seguir:

> [...] verifica-se que 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

[7] Neste sentido, defendem os juristas Maggio (2012) e Cabette (2013).
[8] Neste sentido, interpretam os juristas Greco (2013) e Bitencourt (2013).

> mais grave. Assim sendo, o verbo em questão deve ser entendido como "entrar sem direito ou sem autorização".

Conclui-se, portanto, que a invasão que trata o tipo penal é "virtual"; o núcleo invadir tem o sentido de violar, penetrar, acessar o sistema ou a memória do dispositivo informático.

3.2.3.4.2 Dispositivo informático

Greco (2013) entende por dispositivo informático "todo aquele aparelho capaz de receber dados, tratá-los bem como transmitir os resultados, a exemplo do que ocorre com os computadores, *smartphones, ipads, tablets etc".*

Observa-se que o legislador não apresentou uma lista exaustiva dos aparelhos sujeitos à prática delituosa, mas sim, optou em usar o termo "dispositivo informático" como sendo objeto material da conduta criminosa.

A respeito disso, é interessante a colocação de Cabette (2013), segundo o qual:

> Ao usar a locução "dispositivo informático" de forma genérica, possibilitou a criação adequada de uma norma para a qual é viável uma "interpretação progressiva", ou seja, o tipo penal do art. 154-A, CP é capaz de se atualizar automaticamente sempre que surgir um novo dispositivo informático, o que ocorre quase que diariamente na velocidade espantosa da ciência da computação e das comunicações. Essa espécie de redação possibilitadora de interpretação progressiva é a ideal para essas infrações penais ligadas à informática nos dias atuais, já que, caso contrário, correr-se-ia o risco de que a norma viesse a tornar-se obsoleta no dia seguinte em razão do Princípio da Legalidade Estrita.

Dito isto, conclui-se que qualquer aparelho (incluindo o móvel) que possua a capacidade de armazenar dados ou informações poderá ser considerado dispositivo informático. Dentre estes se destacam os computadores, *notebooks*, *netbooks* e *tablets.* E ainda, os aparelhos celulares dotados de recursos de informática e telemática, tais como os *iphones* e *smartphones.*

3.2.3.4.3 Alheio

O tipo penal exige que o dispositivo informático o qual o agente ingressa seja alheio, ou seja, que pertença a um terceiro, e não à pessoa que o utiliza.

Consentindo, destacam-se os dizeres de Cabette (2013): “É claro que não se poderia incriminar alguém que ingressasse no próprio dispositivo informático; seria como incriminar alguém que subtraísse coisa própria no caso de furto”.

A propósito disso, Cavalcante (2012) chama a atenção dizendo:

> É prática comum entre os *hackers* o desbloqueio de alguns dispositivos informáticos para que eles possam realizar certas funcionalidades originalmente não previstas de fábrica. Como exemplo comum tem-se o desbloqueio do IPhone ou do IPad por meio de um software chamado “Jailbreak”. Caso o *hacker* faça ou invada o sistema de seu próprio dispositivo informático para realizar esse desbloqueio, não haverá o crime do art. 154-A porque o dispositivo invadido é próprio (e não alheio).

Depreende-se que o legislador foi claro ao estabelecer a obrigatoriedade de o dispositivo informático ser alheio para que haja o perfeito enquadramento legal. Logo, se o dispositivo informático for próprio ou coisa abandonada, ou ainda, se a conduta típica for precedida de autorização do titular do dispositivo, o crime será considerado atípico.

3.2.3.5.4 Conectado ou não à rede de computadores

Na maioria das vezes a invasão em dispositivo se procede por meio da rede de computadores, todavia, o legislador admitiu também a possibilidade de ocorrência do crime, ainda que o dispositivo não esteja conectado à internet.

3.2.3.4.5 Mediante violação indevida de mecanismo de segurança

Ademais, o tipo penal exige a existência de um mecanismo de segurança no sistema do dispositivo informático, uma vez que apenas haverá a configuração de crime com a violação indevida deste mecanismo de segurança.

Pode-se definir como mecanismo de segurança:

> [...] todos os meios que visem garantir que somente determinadas pessoas terão acesso ao dispositivo informático, a exemplo do que ocorre com a utilização de *login* e senhas que visem identificar e autenticar o usuário, impedindo que terceiros não autorizados tenham acesso às informações nele contidas. (GRECO, 2013).

Além do *login* e senha, citam-se também como espécies de mecanismos de segurança o antivírus, o *firewall* e a criptografia, conforme estudado no tópico 2.2.4.

3.2.3.4.6 Com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo

Constata-se que o legislador atribuiu uma finalidade especial ao tipo penal em comento, tendo em vista que não bastará a simples invasão, mediante a violação indevida de mecanismo de segurança para se configurar o crime; tal invasão deverá ocorrer com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo.

Entende-se, portanto, que se houver autorização expressa ou tácita do titular do dispositivo, o fato praticado será considerado atípico, não se configurando o crime.

Neste sentido, é relevante a observação trazida por Cabette (2013):

> Para que haja o crime é necessário que ocorra "invasão" indevida mediante violação de mecanismo de segurança. Dessa forma 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. Nesse caso há certamente autorização, no mínimo tácita, de quem de direito, ao acesso a todas as suas informações deixadas em aberto na rede.

Conclui o mesmo autor, dizendo que "obviamente que o técnico informático que supera mecanismo protetor para consertar aparelhagem [também] não comete crime, inclusive porque tem a autorização expressa ou no mínimo tácita do cliente".

Ademais, observa-se que o legislador utilizou os termos dados ou informações como sinônimos a fim de abranger todo e qualquer tipo de conteúdo que a pessoa possa armazenar em um dispositivo informático, sejam fotos, vídeos, arquivos de áudio ou de qualquer outra espécie, mensagens, senhas bancárias, etc.

3.2.3.4.7 Ou com o fim de instalar vulnerabilidades para obter vantagem ilícita

Anota-se que o legislador previu, alternadamente, um segundo especial fim de agir (ou um segundo núcleo de conduta, dependendo do entendimento) qual seja, a instalação de vulnerabilidades visando à obtenção de vantagem ilícita.

Conforme já delineado no segundo capítulo do presente trabalho (tópico 2.2.2), vulnerabilidades de sistema pode ser traduzida como sendo uma espécie de "brecha" em um sistema, normalmente indesejada ou oculta, que pode ser utilizada pelo agente invasor para a execução de *malwares.*

No que concerne à finalidade de obtenção de vantagem ilícita, observa-se que não houve uma restrição por parte do legislador neste tocante.

Assim, traduz-se que a vantagem ilícita pode ser tanto no aspecto econômico (instalação de via de acesso a informações para a obtenção de senhas bancárias) ou de qualquer outra espécie (instalação de vulnerabilidade num computador para obter informações de hábitos e preferências de uma pessoa para o fim de conquistá-la). (CABETTE, 2013).

3.2.3.5 Elemento subjetivo

Configura-se o dolo como elemento subjetivo, o qual deve ser acrescido de um especial fim de agir (dolo específico), conforme preceitua o *caput* do artigo 154-A do Código Penal (BRASIL, 1940).

Atente-se, portanto, que o crime não comporta a modalidade culposa.

3.2.3.6 Classificação doutrinária

Trata-se de crime comum[9], plurissubsistente[10] e comissivo[11]. Comum porque pode ser praticado por qualquer indivíduo; plurissubsistente porque admite tentativa e comissivo porque advém de uma atividade positiva do agente, qual seja, invadir ou instalar. Excepcionalmente poderá ser classificado também como um crime comissivo por omissão[12], ou seja, quando o resultado deveria ser impedido pelos garantes, conforme aduz o § 2º do artigo 13, do Código Penal de 1940 [13]. (MAGGIO, 2012).

É um crime simples, uma vez que tutela um único bem jurídico, qual seja a privacidade da vítima, caracterizada pelo sigilo de dados e informações contidos em dispositivos informáticos de qualquer natureza. (CABETTE, 2013).

---

[9] É o crime que pode ser cometido por qualquer pessoa. A lei não exige nenhum requisito especial. (CAPEZ, 2010, p. 286).

[10] Crime cuja execução pode desdobrar-se em vários atos sucessivos, de tal sorte que a ação e o resultado típico separam-se espacialmente, como é o caso dos crimes materiais, que, em geral, são plurissubsistentes. (BITENCOURT, 2008, p. 214).

[11] Consiste na realização de uma ação positiva visando um resultado tipicamente ilícito, ou seja, no fazer o que a lei proíbe. (BITENCOURT, 2008, p. 212).

[12] No crime comissivo por omissão, a omissão é o meio através do qual o agente produz um resultado. Nestes crimes, o agente responde não pela omissão simplesmente, mas pelo resultado decorrente desta, a que estava, juridicamente, obrigado a impedir (art. 13, § 2º, do CP). (BITENCOURT, 2008, p. 213).

[13] O Código Penal, no artigo 13, § 2º estabelece que o "dever jurídico incumbe a quem: (a) tenha por lei obrigação de cuidado; (b) de outra forma, assumiu a responsabilidade de impedir o resultado; (c) com seu comportamento anterior, criou o risco da ocorrência do resultado". (BRASIL, 1940).

Além disso, é um crime monossubjetivo[14] e instantâneo[15], tendo em vista que pode ser praticado por um único agente (não exigindo concurso) e cuja consumação não se prolonga no tempo. (MAGGIO, 2012).

Classifica-se também como sendo um crime formal[16], uma vez que não exige em seu tipo penal simples um resultado naturalístico para a sua consumação, sendo suficiente a mera invasão ou instalação de vulnerabilidade. Também é formal em sua figura equiparada (CP, art. 154-A, § 1º), pois não exige que o material para a prática delitiva seja realmente utilizado pelo destinatário. (CABETTE, 2013).

Frisa-se, contudo, que no que concerne às figuras qualificadas (CP, art. 154-A, § 3º), não se trata de crime formal, mas sim material[17], porque nestes casos o tipo penal exige que para a consumação do delito, haja a obtenção efetiva de conteúdos ou o controle remoto não autorizado do dispositivo invadido. (CABETTE, 2013).

Por último, considera-se crime penal misto alternativo[18], uma vez que o delito em comento possui dois núcleos de conduta não cumulativos (observa-se pela partícula "ou" presente na redação do tipo penal), senão vejamos.

A primeira conduta é a invasão de dispositivo informático (crime essencialmente doloso), porém que não se perfaz somente com o dolo, exigindo a presença de um elemento subjetivo, qual seja, a obtenção, adulteração ou destruição de dados e informações. A segunda conduta corresponde à instalação de vulnerabilidades com o fim de obter vantagem ilícita.

Anota-se, ainda, que por se tratar de crime penal misto alternativo, o agente poderá incidir em ambos os crimes, desde que num mesmo contexto, respondendo pela prática de apenas um único crime. (CABETTE, 2013).

---

[14] Também classificado como crime unissubjetivo, trata-se daquele que pode ser cometido por uma só pessoa ou por varias, em concurso de agentes. Difere-se, portanto, do crime plurissubjetivo, o qual o tipo penal exige a pluralidade de sujeitos ativos como requisito típico. (ESTEFAM, 2010, p. 83).

[15] É o crime que se esgota com a ocorrência do resultado. […] Instantâneo não significa praticado rapidamente, mas significa que uma vez realizados os seus elementos nada mais se poderá fazer para impedir sua ocorrência. Ademais, o fato de o agente continuar beneficiando-se com o resultado, como no furto, não altera a sua qualidade de instantâneo. (BITENCOURT, 2008, p. 213).

[16] Crime cujo 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. (CAPEZ, 2010, p. 287).

[17] O crime material ou de resultado descreve a conduta cujo resultado integra o próprio tipo penal, isto é, para a sua consumação é indispensável a produção de um dano efetivo. O fato se compõe da conduta humana e da modificação do mundo exterior por ela operada. (BITENCOURT, 2008, p. 213-214).

[18] Conforme explicado no tópico 3.2.3.3 do presente capítulo, esta classificação é definida pelos juristas que entendem que o tipo penal definido no art. 154-A do CP possui duas condutas como núcleo, representadas pelos verbos invadir ou instalar.

3.2.3.7 Consumação e tentativa

Conforme já explicitado, por se tratar de crime formal, a consumação do crime se dá com a mera invasão, não sendo necessária a ocorrência do resultado naturalístico.

Logo, a obtenção, adulteração ou destruição de dados do titular do dispositivo ou a instalação de vulnerabilidades não precisam ocorrer para que o crime se consuma.

No tocante à tentativa, esta também será perfeitamente possível, uma vez que se trata de crime plurissubsistente. Seria o caso, por exemplo, do agente que inicia o procedimento de invasão do computador de um terceiro, porém não consegue violar o mecanismo de segurança do dispositivo. (CAVALCANTE, 2012).

3.2.3.8 Figura equiparada

Nos termos do § 1º, do artigo 154-A, do Código Penal, "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"*. (BRASIL, 1940).

A respeito, Cavalcante (2012) traz como exemplo o caso do "indivíduo que desenvolve um programa do tipo 'cavalo de Tróia' (*trojan horse*), ou seja, um *malware* (*software* malicioso) que, depois de instalado no computador, libera uma porta para que seja possível a invasão da máquina".

Avança o mesmo autor, concluindo que:

> Em alguns cursos de informática, o professor desenvolve *softwares* espiões para testarem a segurança da rede e aprimorarem técnicas de contraespionagem. Há também empresas que elaboram e comercializam tais programas. Obviamente que, em tais situações, não haverá crime considerando que o objetivo não é o de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular, havendo o intuito acadêmico, docente ou de melhorar a segurança das redes empresariais, descobrindo as brechas existentes. O fato seria atípico, portanto, por faltar o elemento subjetivo do injusto. (ob. cit. 2012).

Percebe-se, portanto, a clara intenção do legislador em punir de maneira independente, todo aquele que presta auxílio a um terceiro, facilitando assim a prática do tipo penal previsto no *caput* do artigo 154-A do Código Penal. (BRASIL, 1940).

3.2.3.9 Figura qualificada

O legislador traz no § 3º do artigo 154-A do Código Penal a figura qualificada para o crime em comento. (BRASIL, 1940).

Este parágrafo comina a pena de 6 (seis) meses a 2 (dois anos), acrescida de multa "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".

Buscando entender o significado e o alcance das hipóteses trazidas por esta qualificadora, encontrou-se nos ensinamentos de Cabette (2013, grifo meu) a melhor definição, conforme se pode constatar a seguir:

> O primeiro caso diz respeito a "**comunicações eletrônicas privadas**" como, por exemplo, troca de **e-mails, mensagens SMS, conversas reservadas em redes sociais ou sala de bate papo da internet, trocas de fotos, imagens ou vídeos privados.** Na segunda figura está previsto o caso de violação **de segredos comerciais ou industriais**, o que justifica a exacerbação punitiva, dados os interesses econômicos e negociais que podem ser prejudicados. [...] Já na terceira figura está previsto o acesso a **informações sigilosas**, "assim definidas em lei" (quando o texto se refere a lei não pode haver equiparação a outras espécies normativas como decretos, portarias, resoluções, etc., trata-se de lei em sentido estrito). Aqui se tratam de **informações protegidas por sigilo legal e naturalmente ligadas a órgãos governamentais**, inclusive por questões de segurança nacional. [...] Finalmente há previsão do caso em que a invasão enseje o "**controle remoto não autorizado do dispositivo**" violado. Trata-se [da] denominada **operação de "acesso remoto"** que pode ser implantada legalmente e deliberadamente em empresas, por exemplo, por via de um programa chamado "Team Viewer", o qual possibilita que uma equipe de trabalho tenha acesso, inclusive visual e operacional em tempo real a tudo aquilo que outros colegas estão fazendo em máquinas diversas. Entretanto, tal acesso remoto pode ser realizado de forma clandestina por meio de invasão por um vírus Trojan e então possibilitar ao invasor a manipulação de dados, informações, bem como até mesmo de ações no sistema informático alheio sem ciência ou autorização de quem de direito.

Anota-se, por fim, que a qualificadora é expressamente subsidiária, devendo ser excluída se a conduta do agente for tipificada em crime cominado com pena mais grave. Assim, conclui-se que em caso de conflito de normas penais incriminadoras, prevalecerá a lei a cujo crime for atribuído pena mais grave.

Maggio (2012) exemplifica tal hipótese ao afirmar que "tratando-se de violação de sigilo bancário ou de instituição financeira (Lei 7.492/86, art. 18)[19], o crime é mais grave

[19] Art. 18. Violar sigilo de operação ou de serviço prestado por instituição financeira ou integrante do sistema de distribuição de títulos mobiliários de que tenha conhecimento, em razão de ofício. Pena - Reclusão, de 1 (um) a 4 (quatro) anos, e multa. (BRASIL, 1986).

(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".

3.2.3.10 Causas de aumento de pena

Em análise do tipo penal, anota-se que há a existência de duas espécies de aumento de pena.

A primeira hipótese de aumento de pena incide sobre a figura simples e equiparada. Nos termos do § 2º do artigo 154-A do Código Penal, haverá aumento de pena de um sexto a um terço se da invasão resultar prejuízo econômico, qual seja, dano material ou financeiro. (BRASIL, 1940).

A segunda hipótese de aumento de pena incidirá sobre as figuras qualificadas. Assim, haverá aumento de pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiros dos dados ou informações obtidos pelo agente (CP, art. 154-A, § 4º) ou, ainda, a pena será aumentada de um terço à metade se a invasão for praticada contra as autoridades descritas no § 5º do artigo 154-A, do Código Penal. (BRASIL, 1940).

3.2.3.11 Pena e ação penal

Como visto, a pena prevista para o crime simples (CP, art. 154-A, *caput*), bem como para a figura equiparada (CP, art. 154-A, § 1º) é de detenção de 3 (três) meses a 1 (um) ano e multa. (BRASIL, 1940).

No entanto, se do delito resultar prejuízo econômico para a vítima, o tipo penal prevê em seu § 2º um aumento de pena de um sexto a um terço.

Por último, há a previsão de uma pena maior, de 6 (seis) meses a 2 (dois) anos, e multa, se a invasão objetiva a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais e informações sigilosas.

No tocante à ação penal, em regra, será pública condicionada à representação (CP, art. 154-B, primeira parte). (BRASIL, 1940).

A respeito disso, é sábia a colocação de Cavalcante (2012), como se pode ver no fragmento a seguir:

> [...] Isso se justifica em razão da intimidade e da vida privada serem bens disponíveis e também pelo fato de que a vítima tem o direito de avaliar se deseja

> evitar o processo judicial e assim se proteger contra os efeitos deletérios que podem advir da divulgação das circunstâncias que envolvem o fato [...].

Excepcionalmente, conforme consta na segunda parte da redação do artigo 154-B do Código Penal, a ação será pública incondicionada se o crime for "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". (BRASIL, 1940).

3.3 DEMAIS LEIS ATUAIS RELATIVAS AOS CRIMES INFORMÁTICOS NO BRASIL

3.3.1 Lei n. 12.735/2012 ("Lei Azeredo")

Fruto do polêmico projeto de lei n. 84 (BRASIL, 1999), a Lei n. 12.735 (BRASIL, 2012), popularmente conhecida como "Lei Azeredo" (por conta do nome do deputado relator Eduardo Azeredo), foi publicada juntamente com a Lei n. 12.737, em 03 de dezembro de 2012.

Conforme abordado no tópico 3.1.1, o projeto de lei n. 84 (BRASIL, 1999) possuía um conteúdo polêmico, razão pela foram excluídos a maior parte dos artigos da redação original. Após tramitar por considerável tempo no Senado Federal, sua redação foi reformulada, até culminar na lei n. 12.735 (BRASIL, 2012).

O texto da "Lei Azeredo" determina a retirada imediata de mensagens de conteúdo racista postadas na internet, como já ocorre em outros meios de comunicação tais como televisão, rádio ou materiais impressos.

De mais a mais, a Lei n. 12.735/2012 estabeleceu a criação de delegacias especializadas no combate aos crimes informáticos, determinação esta que, de certa forma fortalece a aplicabilidade da Lei n. 12.737/2012 ("Lei Carolina Dieckmann"), considerando que para a apuração dos crimes informáticos é necessário haver uma perícia altamente complexa, a qual requer aparato técnico-criminal especializado. (BRASIL, 2012).

3.3.2 Lei n. 12.965/2014 (Marco Civil da Internet)

Publicada pelo Diário Oficial da União em 24 de abril de 2014, a Lei n. 12.965, popularmente denominada de Marco Civil da Internet, estabelece princípios, garantias,

direitos e deveres para os usuários da internet no Brasil, motivo pelo qual vem sendo apontada por muitos como uma espécie de Constituição da internet. (BRASIL, 2014).

A recente lei pode ser considerada como um verdadeiro avanço legislativo, pois objetiva regular questões importantes que estavam carentes de orientação normativa, além de estabelecer como princípios básicos a proteção da privacidade, o estabelecimento da neutralidade da rede e a liberdade de expressão em ambiente informático. Ademais, a referida lei delimita a responsabilidade do usuário e do provedor, bem como consolida conceitos importantes que se encontram presentes no atual mundo digital.

Para especialistas, era necessária a aprovação do Marco Civil da Internet a fim de complementar as duas legislações que tipificam crimes na internet ("Lei Carolina Dieckmann" e "Lei Azeredo"), considerando que as regras ali previstas facilitam a apuração da autoria dos crimes informáticos. Nesse viés, Haje (2013) explica:

> A proposta [...] prevê que os provedores de Internet guardem os chamados logs (dados de conexão do usuário, que incluem endereço IP, data e hora do início e término da conexão) por um ano. Como as empresas responsáveis pelo serviço de conexão mantêm cadastros dos internautas, normalmente são capazes de identificar, pelo endereço IP, quem é o usuário.

Sem dúvidas, a aprovação desta lei representa verdadeiro progresso para a sociedade brasileira, principalmente por ser o Brasil um dos países mais ativos na internet atualmente.[20]

[20] O Brasil é o terceiro país em número de usuários ativos na Internet. Em dezembro de 2012, o país ocupava a terceira posição em quantidade de usuários ativos da rede mundial (52,5 milhões), ficando atrás apenas dos Estados Unidos (198 milhões) e do Japão (60 milhões). (FÉ, 2013).

4 A UTILIZAÇÃO DO PRINCÍPIO DA PROPORCIONALIDADE COMO PARÂMETRO REFERIDO AO LEGISLADOR PENAL

Antes de se fazer a análise do crime de invasão de dispositivo informático à luz do princípio da proporcionalidade, é necessário entender o que vem a ser tal princípio, bem como de que forma ele é aplicado no âmbito do Direito Penal.

Este é objetivo do presente capítulo: fazer uma reflexão, de maneira sumária, acerca do princípio da proporcionalidade, perquirindo à aplicação deste pelo legislador penal na cominação dos tipos penais e suas respectivas penas.

4.1 CONCEITO E RELEVÂNCIA DOS PRINCÍPIOS NO ORDENAMENTO JURÍDICO

Os princípios, num contexto geral, possuem o condão de estruturar todo o sistema jurídico. Corroborando, Braga (2004, p. 33) explica que "[...] eles são estruturantes e fundantes do ordenamento jurídico e não apenas meras fontes supletivas de integração do sistema".

Neste sentido, Mello (1980, p. 230) também os define como sendo "[...] mandamento nuclear de um sistema, verdadeiro alicerce dele, disposição fundamental que se irradia sobre diferentes normas compondo-lhes o espírito e servindo de critério para sua exata compreensão e inteligência [...]".

E ainda, nos dizeres de Nucci (2005, p. 25) "*princípio*, no sentido jurídico, significa uma ordenação que se irradia e imanta o sistema normativo, proporcionando alicerce para a interpretação, integração, conhecimento e eficiente aplicação do direito positivo".

Dito isto, é oportuno salientar que o Direito se exprime por meio de normas, que podem ser divididas em: normas-regras e normas-princípios. (ARAÚJO, 2009).

O sistema jurídico-normativo, portanto, constitui-se de princípios e regras, todavia, estes não devem confundir-se, embora não seja simples diferenciar estes dois institutos.

De forma precisa e objetiva, Essado (2008, p. 49-50) assim diferencia estes dois institutos:

> [...] os princípios existem como instrumentos jurídicos para o intérprete e aplicador do Direito diante dos casos concretos. É possível genericamente conceituar os princípios; no entanto, é só a aplicação para casos determinados que lhes dá o verdadeiro alcance, às vezes até inimaginável na teoria. Com as regras a situação é um pouco diferente. Elas podem ou não ser realizadas, de acordo com seu conteúdo.

> Ou a regra vale e, neste caso, deve ser determinado fazer o que ela exige, ou a regra é inválida e não se aplica. [...] É possível concluir que as regras apresentam definição sobre a hipótese e consequência.

Já Estefam (2010, p. 108) ressalta o caráter hierárquico dos princípios, pois defende a ideia de que estes seriam "superiores às regras e constituem sua base e sua *ratio*".

Especificamente na seara penal, Nucci (2005, p. 27), ao explicar sobre a importância dos princípios, assim elucida:

> Extenso deve ser o alcance dos princípios penais, até porque permitem a harmonia do sistema, conferindo coerência às normas criadas pelo legislador, nem sempre com boa técnica e permitindo aplicação sensata. Socorre-se, então, o aplicador do princípio regente para sanar dúvidas e contradições, ultrapassando obstáculos e garantindo que o Direito Penal cumpra seu papel de interventor –embora em caráter subsidiário- nos conflitos existentes em sociedade, punindo os infratores que causaram lesões a bens juridicamente tutelados.

Dada a importância dos princípios conclui-se que, extenso deve ser o seu alcance, principalmente no âmbito do Direito Penal. Isto porque, além de orientarem o legislador em sua atividade, demarcam limites para o aplicador da lei.

4.2 O PRINCÍPIO DA PROPORCIONALIDADE EM SENTIDO AMPLO

Dentre os diversos princípios existentes no ordenamento jurídico, considera-se o princípio da proporcionalidade ferramenta essencial para a atividade interpretativa e aplicativa do Direito.

Acerca de sua importância, Almeida (*apud* BRAGA, 2004, p. 70) destaca que:

> A expressão proporcionalidade tem um sentido literal limitado, pois a representação mental que lhe corresponde é a de equilíbrio: há, nela, a ideia implícita de relação harmônica entre duas grandezas. Mas a proporcionalidade em um sentido amplo é mais do que isso, pois envolve também considerações sobre a adequação entre meios e fins e a utilidade de um ato para a proteção de um determinado direito.

Por conseguinte, constata-se que o significado do termo proporcionalidade está intimamente ligado à ideia de equilíbrio entre dois polos a serem avaliados, seja o bem e o mal, um positivo outro negativo, o muito ou pouco, o meio e fim; em outras palavras, traz a ideia de uma justiça adequada.

4.2.1 Breve escorço histórico

É antiga a ideia de proporcionalidade. Muito embora seja recente a utilização deste princípio pelos operadores do direito, a ideia de proporção está relacionada à aplicação da Justiça desde os primórdios da civilização.

Na Grécia Antiga, a ideia de proporcionalidade se expandiu consideravelmente, considerando a insistente busca do ‘meio termo’ pelo filósofo Aristóteles. A partir do ideário grego, a proporcionalidade avança também em Roma, influenciando o Direito Romano. (ESSADO, 2008).

A ideia de justa medida, difundida por Aristóteles, reaparece e consegue firmar-se durante o período iluminista, notadamente com a obra Dos Delitos e Das Penas, de autoria de Cesare Bonessana, conhecido como Marquês de Beccaria. (GRECO, 2010a, p. 5).

No tocante à utilização da proporcionalidade como forma de limitar à atuação do Estado, suas primeiras manifestações se deram no âmbito do Direito Administrativo, em meados do século XIX, a fim de restringir o livre arbítrio das autoridades através do chamado poder de polícia.

Anota-se, contudo, que a Corte Constitucional Alemã foi a grande propulsora para a inserção do critério da proporcionalidade na esfera constitucional.

Isso porque, com o fim do regime nazista, houve a necessidade de uma legislação que coibisse mazelas semelhantes às decorrentes do regime e que zelasse pelos direitos fundamentais.

A forte utilização do princípio da proporcionalidade na aplicação do Direito Alemão ocasionou a propagação de estudos do tema em toda a Europa, permitindo que países como Áustria, Portugal, Suíça, França, Espanha e Itália desenvolvessem suas leis, doutrina e jurisprudência baseando-se em tal princípio. (BRAGA, 2004).

Por fim, no Brasil, a proporcionalidade também tem sido objeto de estudos em diversos ramos do Direito, conforme será comentado a seguir.

4.2.2 Amparo Constitucional

Apesar de o termo proporcionalidade ter nascido no plano do Direito Administrativo (utilizado com o fim de limitar o poder de polícia), pouco a pouco foi se desenvolvendo em outros ramos da ciência jurídica.

Hodiernamente, encontra-se fortemente inserido no âmbito do Direito Constitucional, e ganha destaque também, na esfera Penal. Insta esclarecer que, o princípio da proporcionalidade não se encontra previsto expressamente na Constituição Federal.

Aragão (2002 *apud* ESSADO, 2008, p. 65-66), neste sentido, explicando sobre a presença do mencionado princípio no ordenamento jurídico, esclarece que:

> É quase unânime a afirmação entre os juristas da existência do princípio da proporcionalidade no ordenamento jurídico brasileiro. Discute-se, todavia, em relação ao seu fundamento. A questão divide-se do seguinte modo: se o fundamento está no direito natural, se é princípio implícito, se integra as bases do Estado Democrático de Direito (CF, art. 1º, *caput*), se advém do princípio do devido processo legal (CF, art. 5º, inc. LIV) ou se é um dos outros princípios constitucionais (CF, art. 5º, § 2º).

Dissensões a parte, é cediço que os princípios jurídicos não precisam estar necessariamente previstos na Constituição Federal (BRASIL, 1988) para ganharem concretude. Basta que haja a possibilidade de extraí-los de outros princípios, tornam-se aplicáveis pelos operadores de direito.[21] É o que ocorre com o princípio da proporcionalidade, cuja observância independe de previsão expressa no texto legal.

Contudo, para o Supremo Tribunal Federal, órgão máximo competente para julgar os casos em que há lesão da Constituição Federal (BRASIL, 1988), o princípio da proporcionalidade advém do princípio do devido processo legal[22] possuindo, assim, matriz constitucional (CF, art. 5º, LIV). [23]

4.2.3 Finalidade e natureza jurídica

A proporcionalidade encontra-se pautada na ideia de limitação do poder estatal, levando-se em consideração a tutela dos interesses individuais. Cabe ao Estado proceder à limitação destes interesses, de modo a atender ao interesse público; a proporcionalidade surge, portanto, como medida de atuação do Estado. (ARAÚJO, 2009).

Criado com o intuito de proteger os direitos fundamentais, Essado (2008, p. 63) ensina que o princípio da proporcionalidade "[...] busca garantir, de um lado a permanência

[21] Tal ideia encontra-se consubstanciada no texto do art 5º, § 2º da CF/1988, *in verbis:* "Os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte". (BRASIL, 1988).

[22] O Supremo Tribunal Federal já se posicionou quanto à origen constitucional do princípio da proporcionalidade, por representar o aspecto do devido processo legal, conforme extrai-se da fundamentação da decisão prolatada na ADI 1158-8, cujo relator foi o Min. Celso de Mello.

[23] Art. 5º, LIV. Ninguém será privado de liberdade ou de seus bens sem o devido proceso legal. (BRASIL, 1988).

do Estado de Direito e, de outro, a limitação de direitos fundamentais, sem restrição absoluta, visando ao bem comum e prevalência do interesse público".

Por encontrar o seu fundamento jurídico na proteção dos direitos fundamentais, o princípio da proporcionalidade é, indubitavelmente, caracterizado como norma constitucional, ganhando *status* de direito fundamental.

4.2.4 Elementos estruturais do princípio da proporcionalidade

O princípio da proporcionalidade possui uma estrutura composta por três elementos, também chamados de subprincípios, quais sejam, a adequação, necessidade e proporcionalidade em sentido estrito.

Araújo (2009) alerta que a análise desses três elementos deve ser feita observando-se uma sequência lógica. Primeiramente, deve-se analisar o subprincípio da adequação, em seguida, o da necessidade e, por último, o juízo da proporcionalidade em sentido estrito.

Estes três subprincípios serão melhor aprofundados, neste trabalho, quando for tratada a aplicação do princípio da proporcionalidade especificamente no campo penal. Por ora, cabe apenas trazer o objetivo principal de tais subprincípios, a saber:

a) adequação – permite sopesar a proporção que deve haver entre o meio escolhido e a finalidade que se pretende obter; deve existir, portanto, coerência entre estes.
b) necessidade – objetiva verificar, como sendo uma espécie de filtro, se a medida escolhida pelo agente estatal para alcançar determinado fim é a mais nociva, dentre as demais medidas existentes.
c) proporcionalidade em sentido estrito – Conhecido pela doutrina como sendo o "princípio da justa medida", este busca o alcance do equilíbrio entre valores e bens. Em outras palavras, diz-se que não basta verificar a adequação e necessidade da medida escolhida pelo agente estatal para alcançar determinada finalidade; é necessário, também, questionar-se quanto ao resultado a ser obtido com a aplicação da medida. Trata-se, portanto, de um juízo de ponderação. (STUMM, 1995).

Como se vê, independentemente do ramo do Direito que tal princípio venha a ser utilizado, sempre terá como meta a aplicação justa da norma. Isso traduz a noção de

equilíbrio, pois impõe limitações para que o indivíduo – enquanto sujeito de direitos –, não seja prejudicado além do permitido, tampouco, favorecido aquém dos limites.

Estabelecidas tais premissas, no próximo item, examinar-se-á o princípio da proporcionalidade especificamente no âmbito Penal.

4.3 O PRINCÍPIO DA PROPORCIONALIDADE NO ÂMBITO DO DIREITO PENAL

4.3.1 Da sua importância

O Direito Penal encontra-se vinculado diretamente com a Constituição Federal (BRASIL, 1988), notadamente em razão do princípio da supremacia da Constituição. Neste sentido, nos dizeres de Essado (2008, p. 25), "[...] o Estado, detentor do direito de punir, encontra na Constituição Federal seus próprios limites".

Nessa mesma linha de raciocínio, Greco (2010b, p. 8) acentua que:

> "[...] não poderá o legislador infraconstitucional proibir ou impor determinados comportamentos sob a ameaça de uma sanção penal, se o fundamento de validade de todas as leis, que é a Constituição não nos impedir de praticar, ou, mesmo, não nos obrigar a fazer aquilo que o legislador nos está impondo".

Por deter o princípio da proporcionalidade guarida constitucional, natural que ocorresse sua ramificação e aplicação por outros ramos do Direito, notadamente o Penal, já que este, é ramo da ciência que se preocupa com a proteção dos bens jurídicos considerados relevantes ao indivíduo e á sociedade.

Dito isto, a partir de agora tal princípio será explanado como princípio fundamental, com enfoque em seu papel delimitador do *jus puniendi* estatal.

4.3.2 Do seu reconhecimento

O princípio da proporcionalidade possui origem na Antiguidade, firmando-se, principalmente, na época do Iluminismo. No entanto, no que cerne ao âmbito penal, o cume de tal princípio adveio com a clássica obra intitulada 'Dos delitos e das penas', publicada em 1764.

Essa obra, de autoria de Cesare Beccaria, despertou na época a importância de se refletir de forma crítica acerca da seara do Direito Penal. E não somente isso; na perspectiva

de Essado (2008, p. 25), "[...] Beccaria associava a proporcionalidade como condição para a realização da justiça penal. O crime necessitava de punição, no entanto, esta não deveria ser abusiva".

Nesse viés, extraem-se da obra de Beccaria (2006, p. 147) os seguintes dizeres: "para que toda pena não seja a violência de um ou de muitos contra o cidadão particular, devendo, porém, ser essencialmente pública, rápida, necessária, a mínima dentre as possíveis, em dadas circunstâncias, proporcional aos delitos e ditadas pelas leis".

A obra de Beccaria, rodeada de inúmeros princípios, dentre eles o da proporcionalidade, serviu e ainda serve como parâmetro para o desenvolvimento de um Direito Penal mais justo e humanitário.

Neste sentido, a própria Declaração Universal dos Direitos do Homem e do Cidadão, de 1789, aderiu às ideias de Beccaria, incorporando-as em seus preceitos normativos. (ESTEFAM, 2010, p. 291). [24]

4.3.3 O princípio da proporcionalidade e a pena

4.3.3.1 A pena no ordenamento jurídico

Derivada do latim *poena*, que significa castigo ou suplício[25], a pena, no passado, tinha um caráter vingativo.

Regressando ao momento histórico em que a pena começou a tomar seus primeiros contornos, anota-se que ela possuía um caráter essencialmente divino. Acreditava-se que os seres divinos castigavam os indivíduos da sociedade, conforme os seus comportamentos. A pena era, portanto, reflexo da vingança divina (Código de Manu), possuindo função reparatória uma vez que o cometimento de delito era considerado pecado.

Ainda em retrospectiva histórica, destaca-se a lei de Talião, acolhida pelo Código de Hamurabi[26], conhecida pela máxima "olho por olho e dente por dente". Nesta, a pena consistia na reciprocidade do crime e da pena, caracterizando uma autêntica vingança

[24] "A lei só deve cominar penas estritamente necessárias e proporcionais ao delito." (Art. 15 da Declaração Universal dos Direitos do Homem e do Cidadão de 1789).
[25] Há quem entenda que o vocábulo pena tem raiz grega (*ponos*), que significa trabalho ou fadiga. (ESTEFAM, 2010, p. 290).
[26] Anota-se que a Lei de Talião também foi incorporada por outras legislações da antiguidade, como a Lei das XII Tábuas dos romanos e o Pentateuco hebreu.

privada.[27]

Com o passar do tempo, a sociedade foi evoluindo e a pena, paulatinamente foi deixando de ter um caráter vingativo – divino ou privado –, passando a ser aplicada pelo Estado.

Nesse sentido, Delmanto et al. (2007, p. 123) explica:

> A função e a razão de ser da pena encontram-se umbilicalmente vinculadas à função e à razão de ser do Direito Penal, como instrumento excepcional e subsidiário de controle social, visando proteger bens considerados essenciais à vida harmônica em sociedade.

No que cerne à finalidade da pena, numa dogmática jurídico-penal, faz-se oportuno transcrever os dizeres de autores renomados do Direito Penal, considerando as diversas teorias existentes acerca dos fins da pena.

Nos dizeres de Greco (2010b, p. 465), "[...] a pena deve reprovar o mal produzido pela conduta praticada pelo agente, bem como prevenir futuras infrações penais".

Para Delmanto et al. (2007, p. 123):

> A pena, enquanto instituto vinculado ao Direito Penal e ao Direito de Execução Penal visa, assim, o futuro. Explica-se: não obstante a punição tenha que se fundamentar na existência de um fato criminoso que comprovadamente provou-se ter ocorrido no passado, mediante o devido processo penal, a pena imposta ao infrator da lei penal, e, sobretudo, a sua execução, tem na ressocialização e na reintegração social do condenado a sua razão de ser.

Sob a perspectiva de Nucci (2005, p. 59):

> A pena, em primeira análise, tem por fundamento e finalidade reafirmar os valores impostos pelas normas vigentes, aquietando o espírito da vítima, para não se voltar contra o delinquente, bem como voltando os olhos à justa punição, que, como já exposto, retribui, previne e busca a ressocialização.

Dito isso, é perceptível que o conceito de pena e sua função propriamente dita encontram-se intimamente ligadas. No entanto, antes de se estabelecer um conceito próprio de pena, é necessário desvelar brevemente acerca das três teorias existentes no tocante às funções da pena. Adiante.

---

[27] No tocante à proporcionalidade, Araújo (2009) esclarece que em que pese tal lei trouxesse consigo uma porção de crueldade e desumanidade na aplicação das penas, a verdade é que "[...] ao preconizar que a reprimenda deveria ser idêntica à lesão perpetrada, a lei do talião institucionalizou a ideia de proporcionalidade entre o delito e a pena [...]".

4.3.3.1.1 A pena como retribuição

Também conhecida como teoria absoluta, a concepção da pena como retribuição está fortemente relacionada à ideia de vingança. A pena, portanto, torna-se "[...] retribuição do mal injusto, praticado pelo criminoso, pelo mal justo previsto no ordenamento jurídico". (CAPEZ, 2010, p. 385).

No tocante à concepção da pena como retribuição, Delmanto et al. (2007, p. 124) rechaça esta teoria, uma vez que "a vingança (que é a essência do retributivismo) é um sentimento que não deve ser nutrido pelo Direito Penal". Para o autor, a pena deve ser aplicada com o fim de prevenção (geral ou especial), a seguir.

4.3.3.1.2 A pena como prevenção geral

Para esta teoria, a pena possui por escopo a reafirmação à sociedade acerca da existência e força do Direito Penal, fortalecendo o poder intimidativo estatal dirigido à sociedade, destinatária da norma penal. (NUCCI, 2005).

Em simples palavras, esta prevenção geral caracterizada pela intimidação social busca fazer com que os indivíduos não cometam mais crimes por medo de serem punidos.

4.2.3.1.3 A pena como prevenção especial

Por derradeiro, tem-se a teoria da prevenção especial da pena, cuja essência encontra-se no caráter reeducativo e ressocializador da pena.

Para Capez (2010, p. 385), "[...] a prevenção é especial porque a pena objetiva a readaptação e a segregação sociais do criminoso como meios de impedi-lo de voltar a delinquir".

E ainda, nos dizeres de Nucci (2005, p. 57), o caráter reeducativo e ressocializador da pena objetiva "[...] preparar o condenado para uma nova vida, respeitando as regras impostas pelo ordenamento jurídico".

4.3.3.2 Definição de pena

Pelo exposto, faz-se agora necessário concretizar a definição de pena, conforme proposto anteriormente.

Nas palavras de Estefam (2010, p. 290), "[...] pena é consequência atribuída por lei a um crime ou a uma contravenção penal. Trata-se de uma sanção, de caráter aflitivo, consistente na restrição a algum bem jurídico, cuja inflação requer a prática de um injusto culpável".

Entretanto, Nucci (2011, p. 401), é quem traz a melhor definição para a pena:

> Sanção do Estado, valendo-se do devido processo legal, cuja finalidade é a repressão do crime perpetrado e a prevenção a novos delitos, objetivando reeducar o delinquente, retirá-lo do convívio social enquanto for necessário, bem como reafirmar os valores protegidos pelo Direito Penal e intimidar a sociedade para que o crime seja evitado.

Sem maiores digressões, passa-se à uma breve exposição dos princípios constitucionais relacionados à pena, que encontram ligação direta com o princípio da proporcionalidade.

4.3.3.3 Princípios regentes da pena que se coadunam com o princípio da proporcionalidade

Os princípios constitucionais penais são de suma importância no ordenamento jurídico penal, uma vez que possuem o *status* de protetores das garantias individuais relacionadas ao indivíduo.

Atualmente, é indispensável que o legislador penal paute-se nos princípios fundamentais previstos na Constituição Federal, bem como obedeça às diretrizes que ordenam o Direito Penal.

Neste contexto, analisar-se-ão alguns princípios regentes da pena: princípio da legalidade, princípio da individualização da pena e princípio da pessoalidade da pena, respectivamente.

4.3.3.3.1 Princípio da legalidade[28]

As penas criminais devem ser previstas em leis, criadas necessariamente antes da conduta do agente e devem possuir conteúdo determinado. Ao magistrado, portanto, não cabe o livre arbítrio para aplicação da pena que entender cabível diante do crime cometido. (ESTEFAM, 2010).

[28] Art. 5º, XXXIX - Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal. (BRASIL, 1988).

4.3.3.3.2 Princípio da individualização da pena[29]

Nas palavras de Estefam (2010, p. 298), "individualizar significa dar tratamento único, especial – tratar o agente como um indivíduo, como uma pessoa única, que cometeu um fato cujas peculiaridades devem ser analisadas".

A individualização da pena atua em três momentos: da cominação, aplicação e da execução da pena. Ao legislador cabe o momento da cominação das penas e de, portanto, cominar penas proporcionais em cada caso concreto.O juiz individualiza a pena no momento da sua aplicação, observando os critérios judiciais previstos no artigo 59 do Código Penal. (BRASIL, 1940).

Por último, no tocante à execução penal, quem possui a função de individualizar a pena neste momento é o juiz da execução penal em conjunto com o próprio pessoal que integra o sistema penitenciário. (BIANCHINI; MOLINA; GOMES, 2009).

Esclarece-se que inclusive na fase executiva, cada preso merece ter tratamento distinto, conforme os preceitos estabelecidos na Lei de Execuções Penais (Lei n. 7.210/1984).

4.3.3.3.3 Princípio da pessoalidade da pena[30]

Este princípio proíbe a imposição de penas por fato de outrem, ou seja, nenhum indivíduo poderá ser punido por fato alheio.

Neste sentido, Capez (2010, p. 385) assinala que inclusive "[...] a pena de multa, ainda que considerada dívida de valor para fins de cobrança, não pode ser exigida dos herdeiros do falecido".

4.3.3.4 A proporcionalidade como parâmetro na criação, interpretação e aplicação dos tipos penais incriminadores

O princípio da proporcionalidade rebate a imposição de cominações legais e a imposição de penas desprovidas de relação valorativa com o fato cometido pelo agente.

---

[29] Art. 5º, XLVI – A lei regulará a individualização da pena e adotará, entre outras, as seguintes: a) privação ou restrição da liberdade; b) perda de bens; c) multa; d) prestação social alternativa; e) suspensão ou interdição de direitos. (BRASIL, 1988).

[30] Art. 5º, XLV – Nenhuma pena pasará da pessoa do condenado, podendo a obrigação de reparar o dano e a decretação do perdimento de bens ser, nos termos da lei, estendidas aos sucessores e contra eles executados, até o limite do valor do patrimonio transferido. (BRASIL, 1988).

Elucidando a ideia acima exposta, Franco (*apud* GRECO, 2010a, p. 5) discorre acerca deste princípio com as seguintes palavras:

> [...] O princípio da proporcionalidade exige que se faça um juízo de ponderação sobre a relação existente entre o bem que é lesionado ou posto em perigo (gravidade do fato) e o bem de que pode alguém ser privado (gravidade da pena). Toda vez que, nessa relação, houver um desequilíbrio acentuado estabelece-se, em consequência, inaceitável desproporção.

Em matéria penal, o princípio da proporcionalidade possui dois destinatários: o Poder Legislativo, o qual deverá estabelecer penas proporcionais à gravidade do delito (proporcionalidade abstrata) e o Poder Judiciário, que deverá impor ao autor do crime pena proporcional à sua gravidade concreta (proporcionalidade concreta).

Há, contudo, quem entenda que tal princípio atinge também um terceiro destinatário: os órgãos responsáveis pela execução penal (proporcionalidade executória). Seguindo esta corrente, Masson (2011, p.43) esclarece que:

> [...] o princípio da proporcionalidade possui três destinatários: o legislador (proporcionalidade abstrata), o juiz da ação penal (proporcionalidade concreta), e os órgãos da execução penal (proporcionalidade executória). Na proporcionalidade abstrata (ou legislativa), são eleitas as penas mais apropriadas para cada infração penal (seleção qualitativa), bem como as respectivas graduações – mínimo e máximo (seleção quantitativa). Na proporcionalidade concreta (ou judicial), orienta-se o magistrado no julgamento da ação penal, promovendo a individualização da pena adequada ao caso concreto. Finalmente, na individualização executória (ou administrativa) incidem regras inerentes ao cumprimento da pena, levando-se em conta as condições pessoais e o mérito do condenado.

Nesse contexto observa-se a importância do princípio da proporcionalidade, sendo ferramenta indispensável a traçar os contornos do *jus puniendi*, seja no aspecto abstrato – relacionado à ação do legislador, ao definir as condutas criminosas e cominar as respectivas penas –, seja no aspecto concreto, direcionado ao intérprete e aplicador da pena.

Apresentadas as formas de utilização do princípio na esfera penal, faz-se oportuno mencionar que o que interessa para o presente estudo, sobretudo, é a fase de predeterminação da lei penal, ou seja, a proporcionalidade com enfoque na atuação do legislador penal na elaboração dos tipos penais e suas respectivas penas.

4.4 O PRINCÍPIO DA PROPORCIONALIDADE E O LEGISLADOR PENAL

Entende-se que a atitude punitiva do Estado em relação à infração deve ser proporcional à gravidade desta infração. Neste sentido, cabe ao legislador penal à missão de fazer a primeira filtragem dos valores previstos no sistema jurídico-constitucional, para assim iniciar o processo de elaboração do tipo penal.

Nesse viés, Nucci (2005, p. 40, grifo meu) afirma que "ao elaborar tipos penais incriminadores **deve o legislador inspirar-se na proporcionalidade**, sob pena de incidir em deslize grave, com arranhões inevitáveis a preceitos constitucionais".

Avança o mesmo autor, esclarecendo acerca da importância do princípio da proporcionalidade no plano legislativo:

> [...] Não teria o menor sentido, levando-se em conta a proteção subsidiária que o Direito Penal deve assegurar aos conflitos sociais, sustentando-se na adequada posição de intervenção mínima, prever penas exageradas para determinados delitos considerados de menor importância, bem como estipular sanções ínfimas para aqueles que visam à proteção de bens jurídicos considerados de vital relevo (ob. cit. 2005, p. 39-40).

Para entender melhor as atitudes legislativas na fase de predeterminação da lei penal, compete avaliar os subprincípios da proporcionalidade já apresentados (adequação, necessidade e proporcionalidade em sentido estrito) em sua ligação direta com o atuar do legislador penal.

4.4.1 O exame da adequação atribuído ao legislador penal

Conforme salientado, um meio será considerado adequado quando se verificar a coerência entre este e a finalidade que se pretende alcançar através dele. Feldens (2005, p. 162) traduz essa 'relação de adequação medida-fim' na realização do interesse público.

Por esse prisma, a adequação atribuída ao legislador penal no tocante à incriminação de condutas deverá prever um juízo de valoração que estabeleça o equilíbrio entre a gravidade das medidas empregadas e a obtenção do resultado que se espera, ou seja, a tutela dos bens jurídicos. (ARAÚJO, 2009).

Nas palavras de Estefam (2010, p. 125), "[...] No campo penal, tal adequação se dará quando ficar evidenciado que a norma regula um comportamento socialmente relevante e referido expressa ou implicitamente em algum valor constitucional". Assim sendo, no que

concerne ao elemento da adequação, se a criminalização da conduta não visar à proteção do bem jurídico, estará caracterizado o abuso por parte do legislador penal.

Desta forma, levando-se em consideração que o subprincípio da adequação encontra-se intimamente atrelado ao bem jurídico, ou melhor dizendo, à efetividade da tutela deste, necessário aprofundar um pouco mais acerca deste.

Em obra aprofundada sobre o tema, Roxin (2006, p. 18-19) define os bens jurídicos como sendo "[...] circunstâncias reais dadas ou finalidades necessárias para uma vida segura e livre, que garanta todos os direitos humanos e civis de cada um na sociedade ou para o funcionamento de um sistema estatal que se baseia nestes objetivos".

Porém, importante assinalar que a preservação da teoria do bem jurídico em nosso ordenamento vem sendo questionada por diversos doutrinadores. Dentre os argumentos existentes, alguns autores entendem que nem todos os crimes constituem ofensa a um bem jurídico, devendo, portanto, não ser considerado como um limite político-criminal. (BIANCHINI; MOLINA; GOMES, 2009).

Para Estefam (2010, p. 42), "o mais importante não é conceituar bem jurídico ou definir se é este, de fato, o escopo do Direito Penal. O verdadeiro desafio do penalista consiste em desvendar quais são os limites do legislador para a criação de normas penais".

Apesar disso, a doutrina majoritária continua admitindo a teoria do bem jurídico tanto como parâmetro limitador da político-criminal , estabelecendo assim uma função de garantia, quanto como referência obrigatória na teoria do delito. (BIANCHINI; MOLINA; GOMES, 2009).

Lado outro, distanciando-se um pouco desta ideia conceitual, e relacionando o bem jurídico ao elemento adequação (subprincípio da proporcionalidade), relevante transcrever os dizeres de Essado (2008, p. 30):

> [...] o trabalho de definir os bens jurídicos não implica solução para estabelecer se determinado comportamento será típico ou não, bem como qual a pena adequada. Mas é imperioso bem definir os contornos sobre os quais os bens jurídicos aptos a receberem a tutela penal transitam. Após isso é que se deve atentar para os critérios que merecem ser utilizados para definir quais condutas podem ser penalmente relevantes, bem como quais espécies e quantidade de penas devem ser previstas abstratamente.

Vê-se, portanto, que o legislador deve estabelecer um critério para definir quais bens são merecedores de tutela penal. O legislador penal não pode escolher aleatoriamente o bem jurídico, nem tampouco indicar todos os bens como sendo jurídicos, uma vez que é necessário haver um equilíbrio.

4.4.2 O exame da necessidade atribuído ao legislador penal

Recapitulando, a análise trifásica do princípio da proporcionalidade atende a uma indispensável sequência lógica. Então, apenas é possível realizar um juízo da necessidade da tutela penal, caso ultrapassado a fase de análise do elemento adequação, ou seja, se constatada a aptidão da tutela penal.

Neste sentido, no que toca ao elemento necessidade, esta examina se, dentre todos os meios disponíveis, o meio utilizado é o menos nocivo e eficaz, para a obtenção do fim pretendido.

Na esfera do Direito Penal, a necessidade da medida encontra-se interligada ao princípio da intervenção mínima (*ultima ratio*) ou subsidiariedade do Direito Penal; isso implica dizer que "não se justificará a utilização deste ramo do Direito quando os demais já apresentam alguma solução satisfatória". (ESTEFAM, 2010, p. 125).

Complementando, Feldens (2005, p. 163) assim elucida:

> Na seara jurídico-penal, devemos indagar se a utilização da norma penal é necessária para alcançar a finalidade de proteção do bem jurídico. A intervenção penal (medida) será necessária se tal finalidade protetiva (fim) não poderia ser conquistada com a mesma eficácia recorrendo-se a uma medida alternativa menos restritiva (sanção civil ou administrativa).

Ultrapassado o exame da necessidade da medida pelo legislador penal, a verificação da proporcionalidade se completará com a análise do subprincípio da proporcionalidade em sentido estrito, a seguir.

4.4.3 O exame da proporcionalidade em sentido estrito atribuído ao legislador penal

Popularmente conhecido como o "princípio da justa medida", a proporcionalidade em sentido estrito, quando verificada no âmbito do Direito Penal, refere-se ao exame da gravidade da sanção a ser imposta diante da conduta praticada pelo agente.

A respeito, Feldens (2005, p. 166) esclarece que o exame deste terceiro elemento da proporcionalidade

> [...] procura determinar se a pena não é desproporcional em seu sentido estrito, que é o que sucede quando se detecta um desequilíbrio patente e excessivo entre a sanção e a finalidade da norma, considerado, no particular, o bem atingido em face de sua incidência (proporcionalidade em sentido estrito).

Em complemento ao que foi transcrito, Araújo (2009) dá destaque ao princípio da proporcionalidade em sentido estrito no momento de elaboração do tipo penal, ao esclarecer que

> [...] deve ser ponderado se a quantidade e a qualidade da pena não possuem o condão de trazer mais desvantagens do que as vantagens que pode proporcionar. [...] o legislador penal não possui o amplo campo de discricionariedade que, prima facie, o princípio da reserva legal confere. Quando da incriminação de condutas, as mazelas, oriundas da aplicação e execução da pena prevista em abstrato, hão de ser sopesadas, em relação à pacificação social que se pretende. De forma mais objetiva, quando da criminalização, para o fim a que se destina o direito penal – tutela subsidiária dos bens jurídicos mais relevantes da sociedade – deve-se aferir os prós e contras.

A política criminal estabelece – através de princípios que orientam e fundamentam a ordenação punitiva – as sanções adequadas para cada tipo de conduta ilícita, bem como provê discrições normativas para que a proporcionalidade possa ser alcançada.

No entanto, deduz-se que há uma certa dificuldade por parte do legislador penal em estabelecer o critério e medida da proporcionalidade no momento de elaboração do tipo penal , principalmente em relação à qualidade e quantidade de pena.

Nos dizeres de Bianchini, Molina e Gomes (2009, p. 398), "o mandato da proporcionalidade implica um juízo lógico ou de ponderação que compara, *valorativamente*, a gravidade do fato antijurídico e a gravidade da pena, a entidade do injusto e a do castigo".

Quanto a este chamado juízo de ponderação, Peña (*apud* BIANCHINNI; MOLINA; GOMES, 2009, p. 398) esclarece que:

> Aqui conta não só a gravidade intrínseca do fato pelo grau de desvalor do resultado e da ação (número e entidade dos bens jurídicos afetados, relevância do dano ocasionado, periculosidade da ação e desvalor da intenção do autor, expressada no fato etc.), senão também a sua gravidade extrínseca, isto é, o perigo de frequência de seu cometimento e conseguinte alarme social, ponto que se pode incluir no desvalor objetivo da ação, se bem que tudo isso só pode ser avaliado com prudência.

Logo, depreende-se que o princípio da proporcionalidade desempenha papel fundamental na limitação do direito de punir do Estado, visando sempre à proteção dos direitos constitucionalmente garantidos aos cidadãos.

5 O CRIME DE INVASÃO DE DISPOSITIVO INFORMÁTICO ACRESCIDO PELA LEI "CAROLINA DIECKMANN" SOB A PERSPECTIVA DO PRINCÍPIO DA PROPORCIONALIDADE

No presente capítulo, objeto central deste estudo, será feita uma análise pormenorizada do crime de invasão de dispositivo informático, previsto no artigo 154-A do Código Penal Brasileiro (BRASIL, 1940), verificando se os critérios utilizados pelo legislador penal no momento da elaboração do tipo e na pena nele cominada atendem, ou não, ao princípio da proporcionalidade.

5.1 A (IN) OBSERVÂNCIA DOS SUBPRINCÍPIOS DA PROPORCIONALIDADE NA REDAÇÃO DO ART. 154-A DO CÓDIGO PENAL

A Lei n. 12.737/2012, então intitulada Lei "Carolina Dieckmann" inseriu os artigos 154-A e 154-B no capítulo referente aos crimes contra a liberdade individual, como já ressaltado no capítulo 3 do presente estudo. (BRASIL, 2012).

Cabe agora, verificar se o legislador na elaboração do preceito secundário da norma obedeceu, ou não ao princípio da proporcionalidade. Para tanto, torna-se imprescindível a filtragem do tipo penal pelos três elementos da proporcionalidade, quais sejam: adequação, necessidade e proporcionalidade em sentido estrito.

Passa-se, portanto, à analise individual de cada elemento normativo presente no artigo 154-A do Código Penal (Invasão de dispositivo informático). (BRASIL, 1940).

5.1.1 Averiguação do subprincípio da adequação

Com relação a este primeiro elemento, verifica-se que agiu com prudência o legislador penal, considerando a relevância do bem jurídico tutelado pelo tipo penal em questão: a liberdade individual. Tanto é verdade, que o aludido tipo penal encontra inserto na seção IV (Dos Crimes Contra a Inviolabilidade dos Segredos), no capítulo VI, do Código Penal, que trata especificamente dos Crimes contra a liberdade Individual. (BRASIL, 1940).

Precisamente, o bem jurídico tutelado pelo artigo 154-A do Código Penal é o da privacidade, que, por sua vez, completa a liberdade individual. (BRASIL, 1940).

Nesse viés, Bitencourt (2013), ao afirmar que a liberdade é parte integrante do direito de privacidade, esclarece que "a proteção da *liberdade* não seria completa se não fosse

assegurado ao indivíduo o direito de manter em sigilo determinados atos, fatos ou aspectos de sua vida, particular e profissional, cuja divulgação pode produzir dano pessoal ou a terceiros, de monta considerável".

Insta esclarecer que o tipo penal em comento não busca proteger a Rede Mundial de Computadores, mas sim a privacidade individual, pessoal e profissional dos indivíduos, que armazenam, cotidianamente, seus dados e informações em dispositivos informáticos. Logo, com acerto o legislador penal, pois não se trata de um novo bem jurídico, mas sim de um já existente no ordenamento e devidamente amparado no texto constitucional.

5.1.2 Averiguação do subprincípio da necessidade

No que se refere à necessidade da medida, também agiu por certo o legislador penal, pois, como já delineado nos capítulos iniciais deste estudo, há tempos se discute sobre a necessidade de tipificação dos intitulados crimes informáticos próprios.

A criação de um tipo penal que abrangesse a conduta de invasão de privacidade a fim de proteger dados e informações armazenados nos dispositivos informáticos (a proteção da chamada segurança informática) era algo indiscutivelmente necessário.

O Brasil, por exemplo, perdeu aproximadamente 8 bilhões de dólares em 2013, com ataques e invasões de hackers, dentre outros crimes informáticos, valor este que representa o percentual de 0,32% do Produto Interno Bruto (PIB) brasileiro. (SCIARRETTA, 2014). Evidentemente, o recrudescimento desta prática delitiva no Brasil, por si só, já justificaria a necessidade de amparo penal.

Mas não só isso; nos dizeres de Bitencourt (2013), "a proteção de dados e dispositivos informáticos e, especialmente, dos conteúdos que (*sic*) armazenam é uma exigência fundamental da atual vida social informatizada, que deve ser respeitada como princípio de ordem pública".

Consequentemente, por deter tal proteção, *status* de ordem pública, fica clara a ideia de que os danos deflagrados pela violação dos dados e dispositivos informáticos não podem ficar apenas resguardados na esfera cível, notadamente no campo da responsabilidade civil. É essencial a responsabilização penal neste tocante, considerando a relevância do bem jurídico que a norma visa proteger, no caso, a intimidade.

Neste sentido, assevera Rodríguez (2008, p. 133) que:

> [...] um sistema que abolisse os direitos da intimidade em prol da tutela exclusivamente civil estaria não só renunciando a uma tarefa evidente do direito penal de proteger bens jurídicos de primeira ordem, como também a desconstituir o grande sentido de injusto que a tipificação confere ao próprio magistrado cível, na absoluta certeza de que a conduta é recriminada socialmente, porque ilícito penal. A intimidade é bem jurídico essencial e necessita da tutela penal.

Desta forma, malgrado se reconheça a intenção de apenas se utilizar o Direito Penal quando os demais ramos da ciência jurídica não se mostrarem suficientes (respeitando assim a diretriz da *ultima ratio*), tal premissa não deve ser utilizada de forma absoluta nos delitos informáticos. Isso porque, conforme já retratado no segundo capítulo, os chamados crimes informáticos próprios necessitavam de tipificação penal por não se enquadrarem em nenhum dos tipos penais já existentes.

Condutas que atentam contra bens informáticos devem ser penalmente criminalizadas em razão ao seu elevado potencial lesivo, notadamente na era digital na qual estamos insertos.

Importante destacar ainda que, apesar da tentativa de se enquadrar a conduta de violação de dispositivo informático na conduta prevista no artigo 10 [31] da Lei n. 9.296/1996 (Lei de interceptação telefônica) [32], entendeu-se que o verbo "interceptar" não poderia abarcar o sentido de invasão e violação de sigilo. (OLIVEIRA, 2011).

Adiciona-se a isto o fato de que com relação à invasão de conteúdo de correspondência eletrônica, havia dificuldade de se enquadrar esta conduta no tipo previsto no artigo 151 [33] do Código Penal (crime de violação de correspondência). Isso porque o artigo 47 da Lei n. 6.538/1978 trouxe o conceito de correspondência, dizendo ser "toda comunicação de pessoa a pessoa, por meio de carta, através de via postal, ou por telegrama." (BRASIL, 1978).

Assim, tendo em vista que a conduta prevista no artigo 151 do Código Penal abarcava somente à correspondência fechada, envelopada ou lacrada, impossível a inserção das mensagens transmitidas por dispositivos informáticos. (OLIVEIRA, 2011).

---

[31] Art. 10 - Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei. (BRASIL, 1996).

[32] A lei de interceptação telefónica (Lei n. 9.296/1996) regulamentou o disposto no inciso XII, parte final, do art. 5º, da Constituição Federal, *in verbis:* "é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal." (BRASIL, 1988).

[33] Art. 151 - Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem.
Pena - detenção, de 1 (um) a 6 (seis) meses, ou multa. (BRASIL, 1940).

Logo, agiu de forma coerente o legislador penal ao buscar tutelar a intimidade resguardada nos referidos bens jurídicos, tipificando a conduta de invasão de dispositivo informático.

5.1.3 Averiguação do subprincípio da proporcionalidade em sentido estrito

Analisando a redação do artigo 154-A do Código Penal (BRASIL, 1940), observa-se a inobservância por parte do legislador no que se refere ao exame do terceiro elemento do princípio da proporcionalidade, qual seja a proporcionalidade em sentido estrito.

Isso porque é importante que a atividade legiferante seja sempre pautada num juízo de ponderação entre a gravidade do delito que se tenta impedir e a quantidade da pena imposta, sob pena de ofensa a princípios fundamentais da Constituição da República. A desproporcionalidade é contrária à justiça penal.

Tal desproporcionalidade se fundamenta por várias razões que serão explanadas a partir de agora.

5.1.3.1 Da desproporcionalidade da pena considerando a gravidade do delito

Usualmente, o princípio da proporcionalidade se traduz como uma proibição de excesso, uma vez que coíbe a cominação de penas por parte do legislador em quantidade exagerada e desnecessária.

Por outro lado, importante frisar que este princípio visa também a impedir a proteção insuficiente de bens jurídicos, ou seja, veda a punição abaixo da medida.
Corroborando, têm-se as palavras de Queiroz (2006, p. 45, grifo meu):

> [...] o princípio da proporcionalidade compreende, além da proibição de excesso, **a proibição de insuficiência da intervenção jurídico penal**. Significa dizer que, se, por um lado, deve ser combatida a sanção desproporcional porque excessiva, por outro lado, **cumpre também evitar a resposta penal que fique muito aquém do seu efetivo merecimento**, dado o seu grau de ofensividade e significação político-criminal, afinal a desproporção tanto pode dar-se para mais quanto para menos.

É com base neste argumento, que se justifica, no presente trabalho, a desproporcionalidade perpetrada pelo legislador ao prescrever as penas do crime de invasão de dispositivo informático (CP, art. 154-A).

Em análise do texto do citado dispositivo, conclui-se que as penas previstas pelo legislador referentes ao crime de invasão de dispositivo informático (CP, art. 154-A) são irrisórias e representam insuficiente proteção para um bem jurídico tão importante, qual seja, a intimidade em ambiente informático. (BRASIL, 1940).

A redação do artigo 154-A criminaliza conduta que objetiva "invadir dispositivo informático alheio, conectado ou não à rede mundial de computadores, mediante violação indevida de mecanismo de segurança".

Como já ressaltado, exige finalidade específica, qual seja "obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita".

A pena cominada para esta conduta é de detenção, de 3 (três) meses a 1 (um) ano, e multa, para as hipóteses previstas no *caput* e do § 1º, as quais serão aumentadas de um sexto a um terço "se da invasão resultar prejuízo econômico".

Anota-se que tal majorante é aplicável somente às figuras descritas no *caput* e no respectivo § 1º, sendo, portanto, inaplicáveis para as hipóteses qualificadas.

Como se vê, o legislador escolheu a detenção como regime inicial de cumprimento de pena privativa de liberdade para o cometimento desta espécie de delito em sua modalidade comum.

A título explicativo, "[...] a pena de reclusão não se confunde com a de detenção, porque aquela pode ser cumprida em qualquer dos regimes penitenciários (fechado, semi-aberto e aberto) e esta, apenas no regime semi-aberto" (FRANCO; STOCO, 2007, p. 236).

O regime semiaberto é caracterizado pela execução da pena em colônia agrícola, industrial ou estabelecimento domiciliar (CP, art. 33, § 1º, b). Nos termos do artigo 35 do Código Penal, devem-se aplicar as regras do regime fechado ao condenado que inicie o cumprimento de sua pena em regime semi- aberto. (BRASIL, 1940).

Nucci (2005, p. 307) alerta que nem todos têm condições de ingressar neste regime, ainda que a pena objetivamente seja igual ou inferior a oito anos, pois cabe ao magistrado, no processo de individualização da pena a verificação no caso concreto da viabilidade da concessão desta espécie de regime.

Já o regime aberto, nos termos da lei, baseia-se na autodisciplina e senso de responsabilidade do condenado, tendo em vista que o condenado deverá, fora do estabelecimento e sem vigilância, trabalhar, frequentar curso ou exercer outra atividade autorizada, permanecendo recolhido durante o período noturno e nos dias de folga (CP, art. 36, § 1º). Ressalta-se ainda que tal regime deverá ser cumprido em Casa do Albergado, que se

caracteriza como sendo prédios situados em centros urbanos, contendo lugares apropriados para os cursos e palestras (NUCCI, 2005).

Assim, é oportuno dizer que essa modalidade de regime, infelizmente, embora tipificado no Código Penal não saiu do plano abstrato. Nesse viés Nucci (2005, p. 308) anota que,

> [...] Por absoluto desdém do Poder Executivo, desde a implementação da Lei de Execução Penal e da nova Parte Geral do Código Penal, não se tem notícia da concretização ideal do regime aberto por todo o Brasil. Especificamente na cidade de São Paulo, onde se concentra o maior número de condenados, inexiste Casa do Albergado, passando o sentenciado a cumprir sua pena em regime inadequado, que é a "prisão albergue domiciliar".

Feitas tais considerações introdutórias, verifica-se que a modalidade de pena privativa de liberdade, inicialmente prevista pelo legislador, se mostra inadequada e ineficaz, quando se leva em consideração o princípio da proporcionalidade em sentido estrito, agregado com a função da prevenção geral da pena.

Isso se deve pelo fato de que a ínfima quantidade de pena cominada pelo legislador dificilmente causará intimidação nos praticantes desta espécie de delito.

Adiciona-se a isso o fato de que a pena máxima cominada ao delito em questão não ultrapassa a dois anos, cumulada ou não com multa, caracterizando uma infração penal de menor potencial ofensivo [34], autorizadora do rito do Juizado Especial Criminal (lei n. 9.099 de 1995) com todos os institutos despenalizadores que lhe são correlatos.

O sujeito, ao invés de ser penalizado com uma pena privativa de liberdade, ainda que na modalidade de detenção, será favorecido com a transação penal [35] e a suspensão condicional do processo.[36]

Para melhor esclarecimento, importante anotar as diferenças existentes entre os benefícios da transação penal e suspensão condicional do processo. É cabível a transação penal nas hipóteses em que a pena máxima abstrata cominada ao delito não ultrapasse a 2

---

[34] Art. 61 - Consideram-se infrações penais de menor potencial ofensivo, para os efeitos desta Lei, as contravenções penais e os crimes a que a lei comine pena máxima não superior a 2 (dois) anos, cumulada ou não com multa. (BRASIL. Lei n. 9.099, 1995).

[35] Art. 98, I - A União, no Distrito Federal e nos Territórios, e os Estados criarão juizados especiais, providos por juízes togados e leigos, competentes para a conciliação, o julgamento e a execução de causas cíveis de menor complexidade e infrações penais de menor potencial ofensivo, mediante os procedimentos oral e sumaríssimo, permitidos, nas hipóteses previstas em lei, a transação e o julgamento de recursos por turmas de juízes de primeiro grau. (BRASIL. Constituição Federal, 1988).

[36] Art. 89 - Nos crimes em que a pena mínima cominada for igual ou inferior a um ano, abrangidas ou não por esta Lei, o Ministério Público, ao oferecer a denuncia, poderá propor a suspensão do processo, por dois a quatro anos, desde que o acusado não esteja sendo processado ou não tenha sido condenado por outro crime, presentes os demais requisitos que autorizariam a suspensão condicional da pena. (BRASIL. Lei n. 9.099, 1995).

(dois) anos e seu encerramento se dá com a aplicação de pena restritiva de direitos ou multa. (SOUSA, 2009).

A suspensão condicional do processo, por sua vez, é cabível nas hipóteses em que a pena mínima cominada ao crime não seja superior a 1 (um) ano. Ademais, este benefício poderá ser aplicado em qualquer procedimento de instrução do processo (comum ou especial), visto tratar-se de um instituto de despenalização, pois "não havendo motivos que justifiquem sua revogação, culmina com a extinção da punibilidade, não havendo imposição de pena" (SOUSA, 2009).

Observa-se ainda que o legislador pátrio estabeleceu uma causa de aumento de pena (de um sexto a um terço) no caso de a invasão resultar em prejuízo econômico. Ademais, o § 3º do artigo 154-A transmudou a espécie de pena privativa de liberdade para a de reclusão (de seis meses a dois anos), acrescida de multa, no caso de a "invasão resultar 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".

Trata-se, na verdade, de uma verdadeira qualificadora, uma vez que além de alterar o patamar da pena base, modificou a modalidade de pena privativa de liberdade para espécie mais gravosa (reclusão), adiante:

> § 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. (BRASIL, 1940, grifo meu).

Interessante notar que o legislador criou especificamente na hipótese do parágrafo 3º (qualificadora) uma nova causa de aumento de pena (§4º), quando houver "divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos".

No que se refere à divulgação de dados ou informações, Bitencourt (2013) pondera:

> *Divulgar*, sem justa causa, conteúdo de *dispositivo informático*, isto é, tornar público ou do conhecimento de um número indeterminado de pessoas esse conteúdo que foi obtido criminosamente, e, por conseguinte, desautorizado por seu titular. A *divulgação* pode produzir-se através de qualquer *meio*, legítimo ou ilegítimo: imprensa, rádio, televisão, internet, exposição ao público, obras literárias etc. Enfim, sempre que haja *comunicação*,

> *informação ou, por qualquer meio,* seja dado a conhecer, a um número indeterminado de pessoas dos **dados ou informações obtidos,** estará consumada a divulgação.

É certo que, a divulgação tem que ser penalizada de uma forma mais contundente quando comparada com a simples invasão. Sobretudo, porque gera consequências irreversíveis às vítimas, principalmente quando a informação é disponibilizada na rede mundial de computadores.

Entretanto, da análise precisa do parágrafo 3º e 4º, conjuntamente com o *caput* do artigo 154-A, percebe-se que a "divulgação, comercialização ou transmissão a terceiro" só funciona como causa de aumento de pena se a invasão for aquela caracterizada pela qualificadora, esquecendo-se o legislador de tipificar a "divulgação, comercialização ou transmissão a terceiro", no caso de a conduta ser praticada nos moldes do *caput* do aludido artigo.

Para melhor compreensão, importante trazer um exemplo prático: se o agente invade dispositivo informático alheio, mediante violação indevida de segurança, obtendo fotos armazenadas em correio eletrônico (conteúdo oriundo de comunicação eletrônica privada, conforme já explicado no tópico 3.2.3.8) e as divulga (CP, art. 154-A, § 4º), abstratamente lhe será infligido uma pena de reclusão de seis meses a dois anos, e multa, acrescida de um a dois terços, conforme o caso. (BRASIL, 1940).

Agora, se esse mesmo agente invadir dispositivo informático alheio, mediante violação indevida de mecanismo de segurança, e obter fotos armazenadas em uma pasta do computador ou do celular (conteúdo que não se enquadra nas espécies previstas no § 3º), e também as divulgar, esta divulgação será atípica por ausência de previsão legal, pois a causa de aumento prevista no § 4º só pode ser aplicada nas espécies de conteúdo previstas pelo parágrafo 3º do mesmo dispositivo legal. Logo, responderá apenas pela invasão e sua pena será de detenção de três meses a um ano, e multa.

Percebe-se, então, uma flagrante desproporcionalidade, pois, no ponto de vista do legislador apenas merecia majoração de pena a divulgação de conteúdo obtido por meio de comunicação eletrônica privada. Mas e as demais formas de obtenção de conteúdo (fotos, arquivos, documentos) armazenado em dispositivos informáticos? A divulgação destes também não seriam merecedores da aludida majorante?

Sendo assim, ao estabelecer uma majorante para os casos de divulgação, comercialização ou transmissão a terceiros, de conteúdo obtido por meio da invasão de dispositivo informático, "esqueceu-se" o legislador de que nem sempre os dados e informações dos quais não se deseja divulgar (devendo manter-se secretos) serão aqueles

armazenados em *e-mails*, ou aqueles frutos de conversa por mensagens de celular ou bate-papo, por exemplo. No tocante às fotografias íntimas, por exemplo, estas poderiam estar armazenadas em uma pasta qualquer do computador, *notebook* ou celular.

Ainda, no que diz respeito à causa de aumento prevista no § 4º [37], considera-se a intenção do legislador em "assegurar a proteção da privacidade e da intimidade do titular do dispositivo informático violado, mantendo secretos fatos ou dados particulares, os quais não se deseja que sejam divulgados ou conhecidos por terceiros". (BITENCOURT, 2013).

Contudo, o texto normativo não conseguiu abarcar hipóteses tão graves quanto às tipificadas, que também careciam de uma pena maior, como a divulgação de fotos íntimas obtidas por meio de dispositivos informáticos, conforme exemplificado. Ademais, observa-se também uma desproporção no *quantum* da pena cominada que, apesar de majorada, não levou em consideração a gravidade do delito praticado.

Explica-se: somente nas hipóteses previstas nos parágrafos 4º e 5º é que a pena máxima cominada ultrapassaria o patamar de 2 (dois) anos , de modo a não ser o agente mais favorecido pela Lei do Juizado Especial Criminal (Lei n. 9.099/1995). No entanto, caberia ainda ao agente a suspensão condicional do processo nos termos do artigo 89 da lei n. 9.099/1995, uma vez que a pena mínima não ultrapassa um ano, nem mesmo considerando os acréscimos máximos aplicáveis. (BRASIL, 1995).

Além disso, apesar de o regime inicial de cumprimento da pena ser reclusão – uma vez que a pena a ser cominada não ultrapassará a 4 (quatro anos) –, o agente poderá cumpri-la em regime de reclusão semi-aberto (se reincidente) ou aberto (se não reincidente), se as circunstâncias judiciais previstas no art. 59 do Código Penal lhe forem favoráveis. (BRASIL, 1940).

Indo mais longe, se estiverem presentes os requisitos previstos no artigo 44 do Código Penal[38], caberá ao agente ter sua pena restritiva de liberdade substituída por pena restritiva de direitos. (BRASIL, 1940).

---

[37] Art. 154-A, § 4º - Nos casos em que houver divulgação, comercialização ou transmissão a terceiro dos dados ou informações obtidos por meio de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou controle remoto não autorizado do dispositivo invadido. (BRASIL, 1940).

[38] Art. 44, *caput* - As penas restritivas de direitos são autônomas e substituem as privativas de liberdade, quando: I - aplicada pena privativa de liberdade não superior a quatro anos e o crime não for cometido com violência ou grave ameaça à pessoa ou, qualquer que seja a pena aplicada, se o crime for culposo; II - o réu não for reincidente em crime doloso; III - a culpabilidade, os antecedentes, a conduta social e a personalidade do condenado, bem como os motivos e as circunstâncias indicarem que essa substituição seja suficiente. (BRASIL, 1940).

Dito isto, o agente que incorrer na conduta prevista pelo artigo 154-A, ainda que tendo sua pena aumentada, conforme o caso, dificilmente estará sujeito ao cárcere. Somente nos casos em que houver a concomitância dos aumentos trazidos pelo § 4º e 5º, é que o patamar, considerando os acréscimos máximos, excederia 1 (um) ano da pena mínima, não sendo admissível sequer a suspensão condicional do processo.

Em conclusão, torna-se claro que, quando mal aplicado pelo legislador o princípio da proporcionalidade no momento da cominação da pena em abstrato, pode resultar numa legislação injusta e ineficiente.

5.1.3.2 Da desproporcionalidade da pena considerando a consequência jurídica do delito

Apesar de a consequência jurídica do delito ser uma das circunstâncias judiciais a ser observada pelo juiz no momento da aplicação da pena base (CP, art. 59), esta também deve ser observada na atividade legiferante. (BRASIL, 1940).

Entende-se por consequência jurídica do crime " [...] a intensidade de lesão ou o nível de ameaça do bem jurídico tutelado. Também diz respeito ao reflexo do delito em relação aos terceiros, não somente ao tocante a vítima". (ESTEFAM, p. 343).

As consequências do delito, especificamente no tipo penal de invasão de dispositivo informático, podem ser traduzidas na ideia de que os prejuízos advindos das condutas ali previstas, dificilmente poderão ser recompostos.

Importante enfatizar que estas consequências podem intensificar-se, quando o alvo do agente criminoso for pessoas jurídicas. Nesse prisma, Crespo (2011, p. 31) explica que:

> No âmbito comercial, grande parte das transações financeiras é feita por computador. No empresarial, muitas empresas guardam eletronicamente seus arquivos mais valiosos. Os sistemas marítimos, aeronáuticos e espaciais, bem como a medicina, dependem em grande parte de sistemas informáticos modernos. As redes informáticas se constituíram como nervos da sociedade, que cada vez mais depende dos computadores e das intranets (redes internas de cada corporação).

Torna-se interessante exemplificar a ideia exposta através de exemplos práticos. Veja-se o caso de uma empresa que, ao se tornar vítima desta espécie de invasão (CP, art. 154-A), venha a ter seus dados contábeis alterados ou danificados ou, ainda, seus termos de negociações e contratos de clientes destruídos. Observa-se, aqui, que os reflexos gerados pela invasão podem se tornar irreversíveis. (BRASIL, 1940).

E não só isso. Por vezes, as consequências oriundas de uma invasão de dispositivo informático não atingem somente a vítima em si (neste caso, a empresa), mas por vezes refletem em terceiros prejudicados[39] que não fazem parte da relação de sujeitos do crime.

Nessa ótica, levando ainda em consideração tal situação hipotética, as consequências da invasão afetariam os fornecedores e clientes da empresa e porque não dizer também os funcionários desta, pois, dependendo da intensidade do prejuízo decorrente da prática delituosa, a empresa teria que realizar demissões a fim de diminuir gastos.

Outra discussão que emerge em relação à conduta tipificada no artigo 154-A do Código Penal é que, em muitas situações, a invasão enquadrada no aludido artigo será apenas um meio (ato preparatório ou etapa do *inter criminis*) para a realização de outro tipo penal. (BRASIL, 1940).

Por tal motivo, é que a pena cominada para o aludido artigo não careceria de tanta relevância, já que, "normalmente, os crimes praticados como meio de atingir um outro são absorvidos por este, pelo Princípio da Consunção. [Assim], apenas na hipótese deste crime final não se consumar é que se pode condenar o agente pelo crime praticado como meio". (GOUVÊA, 1970, p.132).

No entanto, rechaça-se tal argumento, pois nem sempre a invasão de dispositivo informático será um meio de execução para a consumação de outro crime mais gravoso. Há invasões que podem ser realizadas por exclusivo motivo pessoal do agente que, quer por vingança, ou outra motivação (sem ser necessariamente pecuniária), invade um dispositivo informático – quer seja de pessoa física ou jurídica- e destrói ou altera os dados e informações ali contidos.

Ademais, ressalta-se que certos *hackers* efetuam as invasões apenas no intuito de testarem suas habilidades ou mostrarem-se superiores em relação ao grupo social a que pertencem.

As situações expostas demonstram que a invasão ocorrida na forma configurada pelo artigo 154-A do Código Penal, além de constituir um verdadeiro desrespeito à privacidade alheia, gera também sérias consequências às vítimas desta espécie de delito, notadamente quando pessoas jurídicas são atingidas. (BRASIL, 1940).

[39] Embora, de regra, coincidam, na mesma pessoa, as condições de sujeito passivo e prejudicado, podem recair em sujeitos distintos. Aquele é o titular do bem jurídico protegido e, na hipótese, lesado, enquanto este é qualquer pessoa que, em razão do crime, sofre prejuízo ou dano material ou moral; o primeiro será a vítima da relação processual-criminal, e o segundo será testemunha, embora interessada. A relevância da distinção repousa nos direitos decorrentes dessa condição que cada um tem: o sujeito passivo é o titular do direito de representar criminalmente contra o sujeito ativo, além de ter o direito da reparação *ex delicto*; ao prejudicado, por outro lado, resta-lhe o direito de postular a reparação do dano sofrido. (BITENCOURT, 2013).

Considerando que a ação penal no crime de invasão de dispositivo informático somente se procede mediante representação da vítima (salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos), dificilmente a empresa deflagrará o procedimento penal competente, em razão da *strepitus judicis* (escândalo do processo).

Neste sentido, Reis (2012) afirma que a exposição da invasão através da representação judicial por parte das empresas, poderia causar a estas, prejuízos maiores que os próprios prejuízos oriundos da invasão propriamente dita.

Além disso, deve-se levar em consideração que invasões desta espécie podem resultar em altíssimos prejuízos morais e materiais para uma empresa; logo, se tornaria difícil para esta recompor tais prejuízos somente na esfera cível.

Por tal razão, Oliveira (2012) assevera que "[...] somente o direito penal tem o condão de causar expressivo desestímulo no atentado de determinados bens jurídicos, dentre os quais tem se mostrado adequada a inserção da privacidade informática".

Conclui-se, portanto, que as consequências jurídicas deste delito possuem reflexos que extrapolam a esfera individual, atingindo muitas vezes empresas, entidades governamentais e ainda organismos oficiais. Tal conduta merece, portanto, ser penalizada de forma mais contundente considerando os reflexos que produzem na sociedade.

5.1.3.3 Da desproporcionalidade da pena quando comparada a outros tipos penais

Ao cominar uma pena, o legislador deve estabelecer penas que sejam proporcionais ao delito cometido. Deve considerar também as consequências jurídicas do fato delituoso, ou seja, sua nocividade social, e também a culpabilidade do agente.

Sendo assim, espera-se que o legislador não estabeleça penas iguais a delitos de lesividades distintas, nem penas graves a crimes de menor gravidade ou, ainda, penas ínfimas a crimes de maior gravidade.

Nesse pensamento, Ferrajoli (2010, p. 369-370) explica:

> Ainda que seja impossível medir a gravidade de um delito singularmente considerado, é possível, no entanto, afirmar, conforme o principio da proporcionalidade, que do ponto de vista interno se dois delitos são punidos com a mesma pena, é porque o legislador considera-os de gravidade equivalente, enquanto se a pena prevista para um delito é mais severa do que a prevista para outro, o primeiro delito é considerado mais grave do que o segundo. Disso segue-se que se

> do ponto de vista externo dois delitos não são considerados da mesma gravidade ou um estima-se menos grave do que outro, contraria o princípio de proporcionalidade que sejam castigados com a mesma pena ou, pior ainda, o primeiro com uma pena mais elevada do que a prevista para o segundo. Em todos os casos, o princípio da proporcionalidade equivale ao princípio de igualdade em matéria penal.

Em consonância, Capez (2010, p. 40) afirma que,

> Quando a criação do tipo não se revelar proveitosa para a sociedade, estará ferido o princípio da proporcionalidade, devendo a descrição legal ser expurgada do ordenamento jurídico por vício de inconstitucionalidade. Além disso, a pena, isto é, a resposta punitiva estatal ao crime, deve guardar proporção com o mal infligido ao corpo social. Deve ser proporcional à extensão do dano, não se admitindo penas idênticas para crimes de lesividades distintas, ou para infrações dolosas e culposas.

Como se vê, apesar do reconhecimento da importância e necessidade do princípio da proporcionalidade no momento da elaboração da lei penal, é ainda evidente a sua inobservância quando se perquire as penas cominadas em alguns tipos previstos na legislação penal brasileira.

Com efeito, após ser feita uma análise comparativa entre o crime de invasão de dispositivo informático (CP, art. 154-A) e outros tipos penais, constata-se que o legislador penal estabeleceu penas que não condizem com os regramentos impostos pelo princípio da proporcionalidade, conforme se observará adiante. (BRASIL, 1940).

A pena cominada ao delito previsto no artigo 152 do Código Penal (correspondência comercial) fixada em 3 (três) meses a 2 (dois) anos de detenção, o qual a ação criminosa consiste em "abusar da condição de sócio ou empregado de estabelecimento comercial ou industrial para, no todo ou em parte, desviar, sonegar, subtrair ou suprimir correspondência, ou revelar a estranho seu conteúdo" **é maior, no seu máximo**, que a pena para o crime de invasão de dispositivo informático em sua modalidade comum, que é fixada em 1 (um) ano, apenas - sendo que neste último há a inclusão de multa, e naquela não. (BRASIL, 1940).

Infere-se, portanto, que para o legislador: o desvio, sonegação, subtração ou supressão de correspondência comercial possui maior gravidade quando comparada com a invasão de um dispositivo informático, mediante violação indevida de mecanismo de segurança, o que gera uma incongruência jurídica. Apesar de as duas condutas ferirem o mesmo bem jurídico, (intimidade), é patente que a invasão de dispositivo informático alheio é um crime que resulta em consequências muito mais graves dada a amplitude do dano causado.

A desproporcionalidade torna-se mais clara, quando se observa que o crime de invasão de dispositivo informático exige certo grau de conhecimentos técnicos por parte do

sujeito ativo do delito. O aludido tipo penal exige a violação de mecanismo de segurança do dispositivo para configurar o crime; já em relação ao crime de correspondência comercial, basta o desvio, sonegação, subtração ou supressão de correspondência comercial para o crime ser configurado.

No que se refere ao crime de violação de segredo profissional (CP, art. 154), topograficamente situado na mesma Seção do Código Penal que o crime de invasão de dispositivo informático (CP, art. 154-A), consegue-se, claramente, verificar o desequilíbrio entre as duas condutas praticadas e as penas neles cominadas. (BRASIL, 1940).

Não obstante estabeleçam a mesma quantidade de pena em abstrato, é fácil perceber que as condutas possuem consequências jurídicas diversas: uma coisa é revelar a alguém, sem justa causa, segredo de que tem ciência em razão da função, ministério, ofício, ou profissão, causando prejuízos basicamente à vitima afetada. Outra, muito diversa, é invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou ainda instalar vulnerabilidades para obter vantagem ilícita.

Tal impropriedade também é verificada quando o legislador estabelece a mesma pena prevista no crime de invasão de dispositivo informático (detenção, de três meses a um ano, acrescido de multa) aos crimes de charlatanismo (CP, art. 283) e abandono de função pública, quando resultar em prejuízo público (CP, art. 323, § 1º). Para o legislador penal as três espécies de delito possuem a mesma gravidade. (BRASIL, 1940).

Por derradeiro, menciona-se o crime de difamação (CP, art. 139), o qual também possui a mesma pena que o crime de invasão de dispositivo informático em sua forma comum (detenção, de três meses a um ano, acrescido de multa). (BRASIL, 1940).

Chama-se a atenção, aqui novamente para a inobservância do legislador que deixou de prever um aumento de pena para os casos em que houver a divulgação do conteúdo obtido por meio da invasão (conteúdos que não se enquadram nos previstos pelo § 3º do art. 154-A do CP). (BRASIL, 1940).

Conforme já ressaltado, nesse estudo, na hipótese em que o agente divulgar conteúdo que ofenda a reputação da vítima, este receberá pena de detenção, de três meses a um ano, acrescido de multa, previsto no *caput* do artigo 154-A do CP. (BRASIL, 1940).

Isso porque embora se quisesse enquadrar a conduta do agente ao crime de difamação, levando-se em consideração que a divulgação de determinados conteúdos resulta

em flagrante ofensa à honra da pessoa, atente-se que a pena cominada, absurdamente, é a mesma para os dois tipos de delitos.

Anota-se ainda que se a referida difamação ocorresse por meio da internet, a pena seria acrescida de um terço, pois a internet seria considerada mero "meio de facilitação da difamação" (CP, art. 141, III). No entanto, ainda que houvesse tal acréscimo, a pena ali cominada é indubitavelmente desproporcional considerando os resultados a serem produzidos. Cita-se, como exemplo, a divulgação de uma foto íntima na Rede Mundial de Computadores. Seria razoável a aplicação apenas da pena cominada no artigo 141, III do Código Penal? (BRASIL, 1940).

Tais exemplos evidenciam diversos casos em que é perceptível o desequilíbrio entre as cominações penais. O legislador penal prevê penas iguais a delitos que causam menor dano social quando comparados ao crime de invasão de dispositivo informático, ou seja, trata de forma igual situações desiguais.

Pensando nessa problemática, e considerando o crescente número de casos de divulgação de vídeos e fotos íntimas por meio da internet, surgiram, atualmente, cinco projetos de lei acerca do assunto. Dentre eles, destacam-se o PL 6.630 (BRASIL, 2013), apresentado pelo deputado Romário, o qual altera o Código Penal (BRASIL, 1940) tipificando a conduta de "divulgar fotos ou vídeos com cena de nudez ou ato sexual sem autorização da vítima", e ainda o PL 5.555 (BRASIL, 2013), do deputado João Arruda, o qual altera a Lei n. 11.340 (BRASIL, 2006), popularmente conhecida como Lei Maria da Penha, criando mecanismos para o combate a condutas ofensivas contra a mulher no meio da internet. (FRAGA, 2014).

Em conclusão, é evidente a desproporcionalidade que impera na atividade legiferante brasileira que, na maioria das vezes, deixa de observar as garantias expressas na Constituição. (BRASIL, 1988).

5.2 IMPLICAÇÕES NA PRÁTICA JURÍDICA

Além de as penas revelarem-se desproporcionais, há outras circunstâncias que reforçam a incongruência do artigo 154-A do Código Penal (BRASIL, 1940), mormente quando se perquire as implicações na prática para os operadores de direito, conforme se verificará adiante.

5.2.1 Lacunas na redação do art. 154-A do CP que reforçam a preeminente desproporção do tipo penal

Analisando a redação do tipo penal em estudo (CP, art. 154-A), constata-se que além de impor penas desproporcionais ao delito, o legislador pátrio acabou prevendo um tipo penal demasiado abrangente e ambíguo, deixando margens para interpretação penal. (BRASIL, 1940).

A primeira problemática que se infere é acerca da exigência do tipo penal em configurar a invasão de dispositivo informático somente quando houver violação de mecanismo de segurança. Isso implica dizer que nos casos em que houver invasão sem a ocorrência da referida "violação" a conduta seria atípica? Sendo assim, caso o computador esteja completamente desprotegido, não haveria a subsunção fática com o artigo 154-A?

Exemplificando: imagine-se a situação em que uma pessoa que possua um *notebook* desprovido de qualquer espécie de mecanismo de segurança (senha, antivírus, *firewall*). Se um agente invadir este aparelho, com algumas das finalidades previstas no *caput* do artigo 154-A do Código Penal, nesse caso, em razão do princípio da tipicidade, o agente não responderia pelo crime de invasão de dispositivo informático, em virtude da ausência de mecanismo de segurança, situação essa que não se pode aceitar. (BRASIL, 1940).

Indo mais longe, indaga-se: se o pretenso titular do *notebook* esquecê-lo ligado e houver a invasão, de igual forma não restará configurado o crime em comento, por culpa exclusiva da vítima? E a ilicitude da conduta? Não merece punição?

A título exemplificativo, Cavalcante (2012) assevera que "não haverá crime se alguém encontra o *pen drive* (não protegido por senha) de seu colega de trabalho e decide vasculhar os documentos e fotos ali armazenados". Será que tal conduta não seria considerada ilícita? Porque a imoralidade é latente.

Todas as hipóteses aqui destacadas demonstram a inconteste falha do legislador na elaboração do tipo previsto no artigo 154-A do Código Penal. Ainda que o dispositivo informático não esteja protegido por mecanismo de segurança, a lesão ao bem jurídico protegido é visível considerado a privacidade violada. No entanto, tal situação não foi prevista pelo legislador penal. (BRASIL, 1940).

Nesse particular, Capanema (2013, p. 6, grifo meu) complementa tal raciocínio estabelecendo o seguinte comentário crítico:

> Só vai ser crime de invasão se eu invadir um sistema protegido por segurança. Mas o que estamos protegendo não é o sigilo, a privacidade, a intimidade? Então por que só vai ser crime se o computador tiver segurança? **Um computador sem login, sem firewall ou antivírus fica fora da legislação? Isso é um grande erro. É como se o furto de um carro sem alarme não fosse considerado um delito a ser punido.**

Além do mais, o legislador desconsiderou que grande parte dos usuários brasileiros, se esquecem de colocar senhas de acesso em seus computadores. Poucos são aqueles que protegem de maneira efetiva seus dados eletrônicos.

Outra polêmica diz respeito à finalidade especial de obtenção de dados ou informações exigida pelo tipo penal para a configuração do crime. A redação não esclarece se tal obtenção se configura quando o agente copia ou retira dados de um dispositivo informático invadido ou se a simples consulta às informações ali obtidas também configuraria o delito em questão.

Nesse sentido, Rocha (2013) indaga se o indivíduo, de forma dolosa, invade um computador, analisa documentos e imagens da vítima, porém não danifica qualquer documento, tal fato seria considerado atípico?

Por último, destaca-se a discussão que circunda em relação à prática - cada vez mais rotineira - do chamado *phishing scam.*

Consoante já delineado nas primeiras linhas do presente trabalho, tal prática consiste, basicamente, no "o envio de mensagens de *spam* contendo *links* para sites falsos que, ao serem acessados, baixam programas no computador alheio, permitindo devassar dados". (MADUEÑO, 2013).

A discussão que surge diz respeito à possível subsunção fática desta conduta no tipo penal previsto no artigo 154-A do Código Penal (BRASIL, 1940). Isso ocorre porque, até o advento da lei n. 12.737 (BRASIL, 2012), o Superior Tribunal de Justiça vinha enquadrando tal prática no artigo 155, § 4º, II do Código Penal (furto mediante fraude)[40], conforme depreende-se do seguinte julgado:

> CONFLITO NEGATIVO DE COMPETÊNCIA. PENAL E PROCESSO PENAL. **FRAUDE ELETRÔNICA NA INTERNET**. TRANSFERÊNCIA DE NUMERÁRIO DE CONTA DA CAIXA ECONÔMICA FEDERAL. **FURTO MEDIANTE FRAUDE QUE NÃO SE CONFUNDE COM ESTELIONATO**.

[40] Há, contudo, quem entenda que no caso do *phishing scan*, aplica-se o artigo 171 do Código Penal (estelionato), e não o artigo 155 do diploma legal (furto mediante fraude). (PINHEIRO, 2009).

> CONSUMAÇÃO. SUBTRAÇÃO DO BEM. APLICAÇÃO DO ART. 70 DO CPP. COMPETÊNCIA DA JUSTIÇA FEDERAL PARANAENSE. 1. O furto mediante fraude não se confunde com o estelionato. A distinção se faz primordialmente com a análise do elemento comum da fraude que, no furto, é utilizada pelo agente com o fim de burlar a vigilância da vítima que, desatenta, tem seu bem subtraído, sem que se aperceba; no estelionato, a fraude é usada como meio de obter o consentimento da vítima que, iludida, entrega voluntariamente o bem ao agente. 2. Hipótese em que o agente se valeu de fraude eletrônica para a retirada de mais de dois mil e quinhentos reais de conta bancária, por meio da "Internet Banking" da Caixa Econômica Federal, o que ocorreu, por certo, sem qualquer tipo de consentimento da vítima, o Banco. A fraude, de fato, foi usada para burlar o sistema de proteção e de vigilância do Banco sobre os valores mantidos sob sua guarda. Configuração do crime de furto qualificado por fraude, e não estelionato. 3. O dinheiro, bem de expressão máxima da idéia de valor econômico, hodiernamente, como se sabe, circula em boa parte no chamado "mundo virtual" da informática. Esses valores recebidos e transferidos por meio da manipulação de dados digitais não são tangíveis, mas nem por isso deixaram de ser dinheiro. O bem, ainda que de forma virtual, circula como qualquer outra coisa, com valor econômico evidente. De fato, a informação digital e o bem material correspondente estão intrínseca e inseparavelmente ligados, se confundem. Esses registros contidos em banco de dados não possuem existência autônoma, desvinculada do bem que representam, por isso são passíveis de movimentação, com a troca de titularidade. **Assim, em consonância com a melhor doutrina, é possível o crime de furto por meio do sistema informático**. 4. A consumação do crime de furto ocorre no momento em que o bem é subtraído da vítima, saindo de sua esfera de disponibilidade. No caso em apreço, o desapossamento que gerou o prejuízo, embora tenha se efetivado em sistema digital de dados, ocorreu em conta-corrente da Agência Campo Mourão/PR, que se localiza na cidade de mesmo nome. Aplicação do art. 70 do Código de Processo Penal. 5. Conflito conhecido para declarar competente o Juízo Federal de Campo Mourão - SJ/PR. (BRASIL, 2007. Superior Tribunal de Justiça. Terceira Seção. CC 67.343, GO/ Rel: Min. Laurita Vaz. Data do julgamento: 28/03/2007. Data de publicação no DJe: 11/12/2007, grifo meu).

Ressalta-se que, Paulo Teixeira - um dos deputados responsáveis pelo projeto de lei n. 2793 (BRASIL, 2011) que culminou na redação da "Lei Carolina Dieckmann" - afirmou que a prática de *phishing* se enquadraria dentre as condutas tipificadas no art. 154-A do Código Penal. (MADUEÑO, 2013).

Anota-se, porém, a disparidade existente entre as penas cominadas para as duas espécies de crime: o crime de furto mediante fraude (CP, art. 155, § 4º, II) é punido com uma pena de reclusão de 2 (dois) a 8 (oito) anos, acrescido de multa. O crime de invasão de dispositivo informático, conforme mencionado repetidamente, é punido com pena de detenção de 3 (três) meses a 1 (um) ano, acrescido de multa. (BRASIL, 1940).

Acredita-se que, apesar da criação do crime de invasão de dispositivo informático a prática do *phishing scam* continuará sendo caracterizada como crime de furto mediante fraude (CP, art. 155, § 4º, II). (BRASIL, 1940).

Nesse sentido, Cavalcante (2012) assevera:

> [...] o art. 154-A prevê como crime invadir computador, mediante violação indevida de mecanismo de segurança, com o fim de instalar vulnerabilidades para obter

> vantagem ilícita. O art. 155, § 4º, por sua vez, pune a conduta de subtrair coisa alheia móvel (dinheiro, p. ex.) mediante fraude (inclusive por meio virtual). Desse modo, parece que a conduta narrada amolda-se, de forma mais específica e completa, no art. 155, § 4º, sendo o delito do art. 154-A o crime meio para a obtenção da finalidade do agente, que era a subtração. Aplica-se, no caso, o princípio da consunção, punindo o agente apenas pelo furto, ficando a invasão absorvida. Em suma, essa conduta não deixou de ser furto.

Por derradeiro, é necessário dizer que, atualmente, tramita no Congresso o projeto de lei n. 5485 (BRASIL, 2013) de autoria do deputado Eduardo Azeredo, tipificando a prática de *phishing scam* como sendo "estelionato eletrônico", com a criação de mais um inciso a ser acrescido no artigo 171 do Código Penal. (BRASIL, 1940).

Dentre as justificativas do mencionado projeto de lei, ressaltam-se os seguintes dizeres: "[...] uma disposição dessa natureza não foi estabelecida nas recentes legislações editadas sobre o assunto - Lei nº 12.737, de 2012 – conhecida como Lei Carolina Dieckmann, e Lei nº 12.735, de 2012". (BRASIL, 2013).

De qualquer modo, tal informação chama atenção, considerando o pano de fundo que envolveu a promulgação da Lei n. 12.737. (BRASIL, 2012). Explica-se: conforme explicado no terceiro capítulo da presente monografia, a atriz Carolina Dieckmann foi vítima da prática de *phishing.* A atriz cedeu, por vontade e consciência – ainda que induzida a erro – sua senha de *e-mail* aos malfeitores, que a utilizaram a senha enviada pela própria atriz tendo acesso a todos os dados presentes no *e-mail* desta, inclusive as fotos que foram divulgadas.

Levando tais fatos em consideração, ao analisar a conduta praticada no caso Carolina Dieckmann (*phishing*) frente ao tipo penal trazido pela Lei n. 12.737 (BRASIL, 2012), conclui-se que, ainda que já estivesse em vigor a referida lei à época dos fatos, não seria possível enquadrar a conduta dos agentes no tipo penal trazido pela lei.

Grosso modo, diga-se que o artigo 154-A do Código Penal não seria aplicável ao caso "Carolina Dieckmann" que, por sua vez, gerou toda a repercussão dos crimes informáticos e a consequente aceleração da aprovação da lei acerca de tais delitos. (BRASIL, 1940).

Do que foi transcrito, mostra-se desarrazoada a redação do tipo penal em comento, demonstrando que a "Lei Carolina Dieckmann" acabou trazendo para dentro do ordenamento jurídico mais um problema ao invés de uma solução aos denominados crimes informáticos.

5.2.2 A reduzida quantidade de pena prevista no art. 154-A do CP e suas implicações nas fases da persecução criminal

Verificou-se no tópico 5.1.3.1 que, com exceção dos casos previstos nos parágrafos 4º e 5º do artigo 154-A do Código Penal (BRASIL, 1940), a prática do crime de invasão de dispositivo informático implica a competência do Juizado Especial Criminal (Lei n. 9.099/1995), considerado o fato de ser crime de menor potencial ofensivo, já que a pena cominada não ultrapassa 2 (dois) anos. (BRASIL, 1995).

No entanto, é cediço que o procedimento sumaríssimo não comporta a produção de provas complexas em respeito aos princípios da oralidade, simplicidade, celeridade e economia processual. Sendo assim, considerando a exigência de perícia técnica para o crime previsto no artigo 154-A do Código Penal,este delito acaba se tornando incompatível com o rito célere dos Juizados Especiais Criminais. (BRASIL, 1940).

Demais disso, parte dos operadores de direito afirmam que a demora na produção de prova, em muitos casos dará ensejo à a prescrição penal, resultando, assim, na ineficácia da pena. Nesse vértice, corroboram os dizeres de Gomes (2013): "[...] As penas são baixas (em regra, até dois anos), logo, a chance de prescrição é muito grande".

Complementarmente, outro ponto relevante do ponto de vista processual, diz respeito à carência de estrutura e recursos disponíveis nos órgãos competentes para uma rápida investigação e apuração destes crimes.

Desta forma, corrobora Loes (2013):

> A Lei 12.737, portanto, irá requerer uma apuração veloz para funcionar. E isso expõe um dos maiores entraves para seu sucesso: a falta de estrutura para apurar esse tipo de crime. Embora conte com alguns centros de excelência em perícia digital, o Brasil ainda carece de um corpo representativo de profissionais treinados para lidar com esses delitos. Hoje, por exemplo, quem busca a polícia para registrar um boletim desse tipo de ocorrência, pode esperar até três meses para ter seu equipamento periciado.

Albuquerque (2006, p. 189) já enfatizava a necessidade da criação de delegacias especializadas com equipamentos adequados para a apuração dos crimes informáticos, a seguir:

> A questão probatória, um problema considerável nos crimes informáticos, só pode ser bem encaminhada se houver investimento na especialização das polícias. A repressão à criminalidade informática está diretamente associada à criação de uma nova polícia judicial, de uma polícia informática, com formação técnica adequada para detectar e investigar esse tipo de ilícito penal, com equipamentos avançados e

> pessoal treinado para detectar e coletar provas. Também se devem adotar e reforçar mecanismos de cooperação internacional direta.

Por tal razão que a Lei n. 12. 735/2012, vulgo "Lei Azeredo" (BRASIL, 2012) estabeleceu, em seu artigo 4º, a exigência de os órgãos da polícia judiciária estruturarem seus setores e equipes especializadas em prol do combate aos crimes informáticos[41]. No entanto, o referido texto legal deixou de estipular prazos para a efetivação das medidas, deixando assim à disposição de cada Estado a vontade de atender tal determinação.

5.3 CONSIDERAÇÕES CRÍTICAS

O legislador penal, no afã de dar uma resposta concreta à sociedade, por vezes, demonstra certas impropriedades na atividade de legislar. Prova disso foi a atual redação da Lei n. 12.737 (BRASIL, 2012), sobretudo do artigo 154-A, objeto do presente estudo.

Noutro giro, indubitavelmente, a citada Lei representa um verdadeiro avanço legislativo quando se considera a ausência de tipificação específica para os crimes informáticos próprios. Contudo, o legislador, não logrou êxito na elaboração da referia lei penal incriminadora, pois, além de desrespeitar o princípio da proporcionalidade, demonstrou visível desconhecimento da complexidade que abrange os crimes informáticos. De igual modo, o legislador penal não se ateve às questões penais materiais e principalmente processuais quando elaborou a redação do tipo previsto no artigo 154-A do Código Penal. (BRASIL, 1940).

Todavia, não se deseja, aqui, apenas tecer críticas à publicação da lei. Ao contrário. Não se descarta a necessidade da elaboração de norma que tutelassem os crimes informáticos próprios. A questão gira em torno do cenário fático em que se pautou a publicação da "Lei Carolina Dieckmann". (BRASIL, 2012).

É notório que os representantes do Congresso Nacional, principalmente no âmbito penal, quando elaboram leis, caminham simultaneamente às pressões midiáticas que se instauram diante de um certo clamor público.

Sob este aspecto, Gomes, L. F. (2012) explica que:

> O populismo penal midiático sabe que a insegurança (o medo e o rancor coletivos) gera demandas punitivas, que são psicanaliticamente exploradas. Criado o clima geral de insatisfação, de intranquilidade e de incerteza, não resta outro recurso, diz o

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

> legislador, senão editar novas leis penais [...].

O episódio ocorrido com a atriz Carolina Dieckmann influenciou, sem margem de dúvidas, a aceleração dos projetos de crimes informáticos que tramitavam há considerável tempo no Congresso. Porém a pressa do legislador, influenciado pelos meios de comunicação em massa, acabou resultando na elaboração de uma norma incongruente, vaga e desproporcional.

Nesse viés, Capanema (2013, p. 6) reforça dizendo:

> Infelizmente, aproveitaram-se do clamor popular por conta da situação de Carolina Dieckmann [a atriz teve fotos expostas por hacker que queria tirar proveito financeiro] e votaram rapidamente uma legislação complexa. E o resultado não foi bom. Uma lei segundo a qual o infrator terá uma pena de três meses a um ano não irá causar temor ao criminoso.

O caso paradigmático da atriz Carolina Dieckmanna e a elaboração da Lei n. 12.737/2012, trouxe uma ilusão jurídica de que a problemática das invasões em dispositivos informáticos seria resolvida ou ao menos minimizada. (BRASIL, 2012).

Demonstrou-se, por meio do presente estudo que uma lei - ainda que adequada e necessária-, se for confeccionada com carga punitiva insuficiente, viola de forma direta o subprincípio constitucional da proporcionalidade em sentido estrito.

Não se quer, contudo, exacerbar o caráter punitivo dos crimes informáticos próprios, pois se entende que há outros bens jurídicos de igual ou maior relevância que merecem repressão maior por parte do Direito Penal, como é o exemplo dos crimes contra a vida. O que se defende, é o equilíbrio entre a pena cominada e a conduta que nele se pretende punir.

Do que foi visto, o crime previsto no artigo 154-A do Código Penal, não se revela proporcional quando se traça um paralelo entre o bem jurídico tutelado e as consequências jurídicas do crime. (BRASIL, 1940).

Conclui-se, por derradeiro, que a problemática da tipificação criminal de crimes informáticos, principalmente no Brasil, é muito mais complexa do que se imagina. Ainda que se inflijam penas proporcionais ao delito informático, é importante salientar que a simples tipificação penal da conduta ilícita, por si só não é o bastante. É necessária uma política-criminal neste tocante.

Nesse particular, concorda-se com a tese de Vianna (*apud* ROCHA, 2012) ao afirmar que a problemática da prevenção e repressão aos crimes informáticos no Brasil é, antes de tudo, um problema técnico e não jurídico. Avança ainda dizendo:

> De nada vale criarmos leis para reprimirmos os novos crimes se elas não puderem ser aplicadas por falta de treinamento de nossos policiais, de nossos promotores e de nossos magistrados. O melhor meio de se prevenir um crime é indubitavelmente o exemplo dado pela efetiva e correta aplicação da norma repressiva.

Assim também é o pensamento de Rosa (2006, p. 76):

> […] nenhum combate sério aos "crimes de Informática" se esgota no proceso tipificador. Sem a cooperação internacional, sem a melhoria do aparelhamento policial e judicial e sem o aperfeiçoamento profissional dos que operam nessas áreas, a simples existência de uma adequada tipificação não tem o menor significado prático e não basta para tutelar a sociedade contra tão lesiva atividade criminosa.

Consequentemente, é necessário haver uma atuação conjunta entre os órgãos responsáveis nacional e internacionalmente e, principalmente, o rápido aparelhamento policial e judicial a fim de atuarem de forma eficiente e ágil na investigação dessa espécie de crime.

Espera-se que a determinação prevista na "Lei Azeredo" seja cumprida rapidamente, pois na ausência dessa estrutura nas delegacias bem como especialização dos profissionais que atuam no combate ao crime, a Lei n. 12. 737/2012 provavelmente será uma lei sem resultados positivos. (BRASIL, 2012).

Como sugestão, o ideal, do ponto de vista técnico seria que, primeiramente, houvesse a promulgação do Marco Civil da Internet (BRASIL, 2014), a fim de regular várias outras questões importantes acerca da Rede, bem como a "Lei Azeredo" (BRASIL, 2012), a fim de estabelecer a readequação e instalação de delegacias especializadas ao combate ao crime. Após, é que deveria ter sido publicada leis que criminalizassem condutas ainda não abarcadas pela legislação penal até então vigente.

Levando-se em consideração a forma em que se procedeu as edições das referidas leis, conclui-se que hoje, no Brasil, apesar da existência de lei repressora, inexiste lei funcional no tocante aos crimes informáticos próprios. E este é o prejuízo causado pelo imediatismo da nova legislação em comento.

5 CONCLUSÃO

Com o presente trabalho, verificou-se que, apesar da intenção do legislador penal em elaborar uma lei repressora aos crimes informáticos próprios, este acabou por redigir um texto penal o qual se tornou alvo de embates entre os operadores de direito atuantes das áreas de Direito Penal e Direito Eletrônico.

Importante salientar que, infelizmente, no Brasil, há uma "cultura" do Poder Legislativo em elaborar leis que atendam – de forma rápida – ao clamor público, influenciado, na maioria das vezes, pelo sensacionalismo da mídia. Neste sentido, conclui-se que uma lei produzida às margens do imediatismo legislativo dificilmente trará resultados positivos, conforme se verificou através da análise da redação do artigo 154-A, acrescido ao Código Penal pela "Lei Carolina Dieckmann".

Desse modo, a resposta ao problema formulado no início deste estudo deve ser no sentido de que houve uma inobservância do legislador às diretrizes do chamado princípio da proporcionalidade ao tipificar a conduta de "invasão de dispositivo informático".

Atualmente, muitos dados e informações são arquivados em dispositivos informáticos e a invasão destes sistemas permite que o agente criminoso tenha acesso a informações pessoais e profissionais dos indivíduos. No entanto, o legislador penal impôs uma ínfima quantidade de pena em abstrato para uma conduta de grande relevância e que merece ser protegida pela lei.

Além disso, o tipo penal trazido pela Lei n. 12.737/2012 (crime de invasão de dispositivo informático) trouxe dúvidas atinentes à sua redação e à sua forma de aplicação no caso concreto, bem como demonstrou dificuldade no tocante à persecução criminal desta espécie de delito.

Como se vê, várias questões foram levantadas sem que se pudesse chegar a uma resposta definitiva. A razão disto é clara: por se tratar de um tipo penal recente, seus efeitos ainda não puderam ser sentidos de forma consistente na prática. Logo, a única certeza que se tem é que somente a evolução da jurisprudência, no caso concreto, poderá solucionar tal problemática.

Diante deste quadro, espera-se que futuros projetos de leis no tocante a crimes informáticos sejam redigidos de uma melhor maneira, levando em consideração a realidade do meio informático e da Rede, pois, caso contrário, o Brasil permanecerá na posição em que se encontra hoje: um país às margens da criminalidade informática e carente de lei funcional neste tocante.

REFERÊNCIAS

ALBUQUERQUE, Roberto Chacon de. **A criminalidade informática**. São Paulo: Juarez de Oliveira, 2006.

ARAS, Vladimir. Crimes de informática. Uma nova criminalidade. **Jus Navegandi,** Teresina, ano 6, n. 51, 1 out. 2001. Disponível em: <http://jus.com.br/revista/texto/2250 >. Acesso em: 17 abr. 2014.

ARAÚJO, Fábio Roque da Silva. O princípio da proporcionalidade aplicado ao direito penal: fundamentação constitucional da legitimidade e limitação do poder de punir. **Revista da EMERJ**, Rio de Janeiro, v. 12, n. 45, p. 273-315, 2009. Disponível em: < http://www.emerj.tjrj.jus.br/revistaemerj_online/edicoes/revista45/Revista45_273.pdf>. Acesso em: 10 maio 2014.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:** Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2006.

BATISTA, Emerson de Oliveira. **Sistemas de informação**: o uso consciente da tecnologia para o gerenciamento. São Paulo: Saraiva, 2006.

BECCARIA, Cesare. **Dos delitos e das penas**. Tradução: J. Cretella Jr. e Agnes Cretella. 4. ed. São Paulo: Revista dos Tribunais, 2006.

BIANCHINI, Alice; MOLINA, Antonio García-Pablos de; GOMES, Luiz Flávio. **Direito penal:** introdução e princípios fundamentais. v.1. 2. ed. São Paulo: RT, 2009. v. 1

BITENCOURT, Cezar Roberto. **Tratado de direito penal:** parte geral, v. 1. 13. ed. São Paulo: Saraiva, 2008.

_____. Invasão de dispositivo informático. **Atualidades do direito**. São Paulo, 7 fev. 2013. Disponível em:<http://http://atualidadesdodireito.com.br/cezarbitencourt/2012/12/17/invasao-de-dispositivo-informatico/>. Acesso em: 23 maio 2014.

BORGES, Walesca; WENECK, Antônio. **Caso Carolina Dieckmann:** polícia busca suspeitos de divulgação de fotos. Disponível em: <http://oglobo.globo.com/rio/casocarolina-dieckmann-policia-busca-suspeitos-de divulgacao-de-fotos 4828719#ixzz2QgD9FCp7>. Acesso em: 14 abr. 2014.

BRAGA, Valeschka e Silva. **Princípios da proporcionalidade e da razoabilidade.** Curitiba: Juruá, 2004.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988. Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 07 maio 2014.

_____. Decreto-Lei nº 2.848, de 07 de dezembro de 1940. **Código Penal.** Disponível em <http://www.planalto.gov.br/ccivil_03/decretolei/Del2848compilado.htm>. Acesso em 14 abr. 2014.

_____. **Lei nº 7.210, de 11 de julho de 1984.** Institui a Lei de Execução Penal. Disponível

em: <http://www.planalto.gov.br/ccivil_03/leis/l7210.htm>. Acesso em: 30 maio 2014.

_____. **Lei nº 7.492, de 16 de junho de 1986.** Define os crimes contra o sistema financeiro nacional, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/l7492.htm>. Acesso em: 30 maio 2014.

_____. **Lei nº 9.099, de 26 de setembro de 1995.** Dispõe sobre os Juizados Especiais Cíveis e Criminais e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9099.htm>. Acesso em: 14 mar. 2014.

_____. **Lei nº 9.296, de 24 de julho de 1996.** Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9296.htm>. Acesso em: 14 mar. 2014.

_____. **Lei nº 11.340, de 7 de agosto de 2006.** Cria mecanismos para coibir a violência doméstica e familiar contra a mulher, nos termos do § 8º do art. 226 da Constituição Federal, da Convenção sobre a Eliminação de Todas as Formas de Discriminação contra as Mulheres e da Convenção Interamericana para Prevenir, Punir e Erradicar a Violência contra a Mulher; dispõe sobre a criação dos Juizados de Violência Doméstica e Familiar contra a Mulher; altera o Código de Processo Penal, o Código Penal e a Lei de Execução Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11340.htm>. Acesso em: 19 maio. 2014.

_____. **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. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acesso em: 14 mar. 2014.

_____. **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. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 14 mar. 2014.

_____. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 30 maio 2014.

_____. **Projeto de Lei nº 84/1999.** Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028>. Acesso em: 30 abr. 2014.

_____. **Projeto de Lei nº 2793/1989.** Dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=529011>. Acesso em: 30 abr. 2014.

_____. **Projeto de Lei nº 5485/2013.** Dispõe sobre a tipificação criminal do estelionato informático. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=A619D81A0CA3852EFD5324B26D3C3A1E.proposicoesWeb1?codteor=1084535&filename=PL+5485/2013>. Acesso em: 30 maio. 2014.

_____. **Projeto de Lei nº 5555/2013.** Altera a Lei nº 11.340, de 7 de agosto de 2006 - Lei Maria da Penha - criando mecanismos para o combate a condutas ofensivas contra a mulher na Internet ou em outros meios de propagação da informação. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1087309&filename=PL+5555/2013>. Acesso em: 30 maio. 2014.

_____. **Projeto de Lei nº 6630/2013.** Acrescenta artigo ao Código Penal, tipificando a conduta de divulgar fotos ou vídeos com cena de nudez ou ato sexual sem autorização da vítima e dá outras providências. Disponível em: < http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=598038>. Acesso em: 30 maio. 2014.

_____. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 1158-8**. Relator: Min. Celso de Mello, DF, 19 de dezembro de 1994. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=346863>. Acesso em: 30 abr. 2014.

_____. Superior Tribunal de Justiça. **Conflito de competência nº 67.343**. Relator: Min. Laurita Vaz, DF, 11 de dezembro de 2007. Disponível em: <https://ww2.stj.jus.br/revistaeletronica/Abre_Documento.asp?sSeq=675605&sReg=200601661530&sData=20071211&formato=PDF>. Acesso em: 30 maio. 2014.

_____. Supremo Tribunal Federal. **Habeas Corpus nº 76689**. Relator: Min. Sepúlveda Pertence, DF, 22 de setembro de 1998. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=76856>. Acesso em: 30 maio 2014.

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/revista/texto/23522>. Acesso em: 22 abr. 2014.

CAPANEMA, Walter Aranha. Cibercriminoso não vai para a cadeia no Brasil. **Convergência digital**, n. 4, p. 4-8, abr/maio 2013. Disponível em: < http://issuu.com/convergenciadigital/docs/revista_04>. Acesso em: 10 maio 2014.

CAPEZ, Fernando. **Curso de direito penal:** parte geral, v. 1. 14. ed. São Paulo: Saraiva, 2010.

CARLI, Daniel Michelon de. **Crimes virtuais no Brasil** – Uma análise jurídica. Santa Maria: UFSM, 2006. Disponível em: <http://www.usr.inf.ufsm.br/~dcarli/elc1020/artigo-elc1020.pdf>. Acesso em: 22 mar. 2014.

CARTILHA DE SEGURANÇA PARA INTERNET. São Paulo: Comit, 2012. Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 30 maio 2014.

CASTRO, Carla Rodrigues Araújo de. **Crimes de informática e seus aspectos processuais.** 2. ed. Rio de Janeiro: Lumen Juris, 2003.

CAVALCANTE, Márcio André Lopes. **Primeiros comentários à Lei n.°12.737/2012, que tipifica a invasão de dispositivo informático.** Disponível em: <http://www.dizerodireito.com.br/2012/12/primeiros-comentarios-lei-127372012-que.html>. Acesso em: 27 abr. 2014.

CORRÊA, Gustavo Testa. **Aspectos jurídicos da internet**. São Paulo: Saraiva, 2000.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais.** São Paulo: Saraiva, 2011.

DECLARAÇÃO UNIVERSAL DOS DIREITOS DO HOMEM E DO CIDADÃO DE 1789. Assembleia Nacional Constituinte. 26 agosto 1789. Disponível em: <http://www.historianet.com.br/conteudo/default.aspx?codigo=180>. Acesso em: 03 maio 2014.

DELMANTO, Celso et. al. **Código penal comentado**. 7. ed. Rio de Janeiro: Renovar, 2007.

ESSADO, Tiago Cintra. **O princípio da proporcionalidade no direito penal**. Porto Alegre: Sergio Antonio Fabris Editor, 2008.

ESTEFAM, André. **Direito penal**: parte geral, v. 1. São Paulo: Saraiva, 2010.

FÉ, Ana Lúcia Moura. **Brasileiros são os campeões mundiais em tempo gasto na internet, segundo ibope.** 2013. Disponível em: <http://www.webexpoforum.com.br/19/02/2013/brasileiros-sao-os-campeoes-mundiais-em-tempo-gasto-na-internet-segundo-ibope/>. Acesso em: 06 jun. 2014.

FELDENS, Luciano. **A Constituição penal:** a dupla face da proporcionalidade no controle de normas penais. Porto Alegre: Livraria do Advogado, 2005.

FERRAJOLI, Luigi. **Direito e razão:** teoria do garantismo penal. 3. ed. São Paulo: Revista dos Tribunais, 2010.

FRAGA, Vitor. PL criminaliza divulgação de vídeos e fotos íntimas na internet. **Tribuna do advogado.** Rio de Janeiro, 2014. Disponível em : <http://www.oabrj.org.br/materia-tribuna-do-advogado/18053-Intimidade-que-fere>. Acesso em: 26 maio 2014.

FRANCO, Alberto Silva; STOCO, Rui (coord.). **Código penal e sua interpretação**: doutrina e jurisprudência. 8ª ed. São Paulo: Revista dos Tribunais, 2007.

GIL, Antônio Carlos. **Métodos e Técnicas de Pesquisa Social**. 6. ed. São Paulo: Atlas, 2008. Disponível em: <http://ayanrafael.files.wordpress.com/2011/08/gil-a-c-mc3a9todos-e-tc3a9cnicas-de-pesquisa-social.pdf.>. Acesso em: 12 jun. 2014.

GOMES, Luiz Flávio. Lei "Carolina Dieckmann" e sua (in)eficácia. **Jus Navigandi**, Teresina, ano 18, n. 3536, 7 mar. 2013. Disponível em: <http://jus.com.br/revista/texto/23897>. Acesso em: 16 mar. 2013.

_____. Populismo penal e inflação legislativa. **O documento**, Cuiabá, out. 2012. Disponível em: <http://www.odocumento.com.br/artigo.php?id=3168>. Acesso em: 03 jun. 2014.

GOMES, Marcelo. Cinco hackers são suspeitos de divulgar fotos de atriz. **Estadão.** São Paulo, 14 maio 2012. Disponível em: <http://www.estadao.com.br/noticias/geral,cinco-hackers-sao-suspeitos-de-divulgar-fotos-de-atriz,872943,0.htm>. Acesso em: 26 abr. 2014.

GÔUVEA, Sandra. **O direito na era digital**: crimes praticados por meio da informática. Rio de Janeiro: Mauad, 1997.

GRECO, Rogério. Invasão de dispositivo informático – art. 154- A do Código Penal. **Atualidades do direito.** São Paulo, 8 jan. 2013. Disponível em: < http://atualidadesdodireito.com.br/rogeriogreco/2013/01/08/invasao-de-dispositivo-informatico-art-154-a-do-codigo-penal/>. Acesso em: 27 abr. 2014.

_____. **Código penal comentado**. 4. ed. Rio de Janeiro: Impetrus, 2010a.

_____. **Curso de direito penal:** parte geral. 12. ed. Rio de Janeiro: Impetus, 2010b.

HAJE, Lara. **Aumenta polémica em torno de projeto de crimes na internet**. Brasília, jul. 2011. Disponível em: <http://www2.camara.leg.br/camaranoticias/noticias/CIENCIA-E-TECNOLOGIA/199811-AUMENTA-POLEMICA-EM-TORNO-DE-PROJETO-DE-CRIMES-NA-INTERNET.html>. Acesso em: 31 maio 2014.

_____. **Marco civil da internet complementará leis de crimes virtuais, dizem especialistas**. Brasília, mar. 2013. Disponível em: < http://www2.camara.leg.br/camaranoticias/noticias/CIENCIA-E-TECNOLOGIA/437714-MARCO-CIVIL-DA-INTERNET-COMPLEMENTARA-LEIS-DE-CRIMES-VIRTUAIS,-DIZEM-ESPECIALISTAS.html>. Acesso em: 31 maio 2014.

LAUDON, Kenneth C.; LAUDON, Jane P. **Sistemas de informação gerenciais.** Tradução Thelma Guimarães. 7. ed. São Paulo: Prentice Hall, 2007.

LOES, João. Lei Carolina Dieckmann: apenas o primeiro passo. **Istoé independente**, n. 2264, abr. 2013. Disponível em: <http://www.istoe.com.br/reportagens/288575_LEI+CAROLINA+DIECKMANN+APENAS+O+PRIMEIRO+PASSO >. Acesso em: 29 maio. 2014.

MADUEÑO, Denise. Projeto torna crime invasão de computador. **Estadão.** São Paulo, 15 maio 2012. Disponível em: <http://www.estadao.com.br/noticias/geral,projeto-torna-crime-invasao-de-computador,873432,0.htm>. Acesso em: 27 maio 2014.

MAGGIO, Vicente de Paula Rodrigues. Novo crime: Invasão de dispositivo informático – CP, art. 154-A. **Atualidades do direito**. São Paulo, 16 dez. 2012. Disponível em: < http://atualidadesdodireito.com.br/vicentemaggio/2012/12/16/invasao-de-dispositivo-informatico-cp-art-154-a/>. Acesso em: 27 abr. 2014.

MASSON, Cleber Rogério. **Direito penal esquematizado**: parte geral, v. 1. 4. ed. São Paulo: Método, 2011.

MAZZARDO, Luciane de Freitas; GÖSSLING, Luciana Manica. A proteção de direitos fundamentais à luz da tipificação de novos crimes cibernéticos. In: Congresso Internacional de Ciências Criminais, 4, 2013, Porto Alegre. **Anais eletrônicos...** Disponível em: <http://ebooks.pucrs.br/edipucrs/anais/cienciascriminais/IV/07.pdf>. Acesso em: 10 mar. 2014.

MELLO, Celso Antônio Bandeira de. **Elementos de direito administrativo**. São Paulo: Revista dos Tribunais, 1980.

MOTTA, Alexandre de Medeiros. **Metodologia da pesquisa jurídica.** Tubarão: Copiart, 2012.

NOGUEIRA, Sandro D'Amato. **Crimes de informática.** São Paulo: BH Editora, 2008.

NUCCI, Guilherme de Souza. **Individualização da pena.** São Paulo: Revista dos Tribunais, 2005.

_____. **Manual de direito penal:** parte geral e parte especial. 7. ed. São Paulo: Revista dos Tribunais, 2011.

OLIVEIRA, Tainá Cristina de. **Privacidade na internet à luz do direito penal.** 2012. 134 f. Monografia (Graduação em Direito) – Universidade Estadual do Norte do Paraná, Jacarezinho, 2012. Disponível em: <http://pt.scribd.com/doc/137134742/TCC-Taina-Cristina-de-Oliveira-Privacidade-na-internet-a-luz-do-Direito-Penal>. Acesso em: 25 abr. 2014.

OLIVEIRA, Fernando José Vianna. Crimes previstos no arts. 150 a 154 do Código Penal e o conflito aparente de normas. **Conteúdo Jurídico**, Brasília: 20 jun. 2011. Disponível em: <http://www.conteudojuridico.com.br/?artigos&ver=2.32489&seo=1>. Acesso em: 29 maio 2014.

PENIDO, Flávia. Os crimes previstos na Lei Dieckmann. **Canaltech Corporate**. São Paulo, 11 abr. 2013. Disponível em: <http://corporate.canaltech.com.br/noticia/juridico/Os-crimes-previstos-na-Lei-Dieckmann/>. Acesso em: 26 abr.2014.

PINHEIRO, Patrícia Peck. **Direito Digital**. 3ª Edição. São Paulo: Saraiva. 2009.

QUEIROZ, Paulo. **Direito penal:** parte geral. 3. ed. São Paulo: Saraiva, 2006.

REIS, Rogério. Novas leis contra crimes cibernéticos, velhos problemas. **Webinsinder**, dez. 2012. Disponível em: < http://webinsider.com.br/2012/12/10/novas-leis-contra-crimes-ciberneticos-velhos-problemas/#sthash.VJ48ulEq.dpuf>. Acesso em: 20 maio 2014.

ROCHA, Carolina Borges. A evolução criminológica do Direito Penal: Aspectos gerais sobre os crimes cibernéticos e a Lei 12. 737/2012. **Jus Navigandi**, Teresina, ano 18, n. 3706, 24 ago. 2013. Disponível em: <http://jus.com.br/artigos/25120>. Acesso em: 24 abr. 2014.

RODRIGUEZ, Victor Gabriel. **Tutela Penal da Intimidade:** Perspectivas da atuação penal na sociedade da informação. São Paulo: Atlas, 2008.

ROSA, Fabrízio. **Crimes de informática.** 2. ed. Campinas: Bookseller, 2006.

ROXIN, Claus. **A proteção de bens jurídicos como função do Direito Penal**. Org. e trad. André Luís Callegari e Nereu José Giancomolli. 2. ed. Porto Alegre: Livraria do Advogado, 2009.

SCIARRETTA, Toni. Brasil perde até U$ 8 bilhões com crime cibernético. **Folha de S. Paulo.** São Paulo, jun. 2014. Disponível em: <http://www1.folha.uol.com.br/mercado/2014/06/1467110-brasil-perde-ate-us-8-bilhoes-com-crime-cibernetico.shtml>. Acesso em: 10 jun. 2014.

SIENA, David Pimentel Barbosa de. Lei Carolina Dieckmann e a definição de "crimes virtuais". **Jus Navigandi**, Teresina, ano 18, n. 3652, 1 jul. 2013. Disponível em: <http://jus.com.br/artigos/24406/lei-carolina-dieckmann-e-a-definicao-de-crimes-virtuais#ixzz30UgVXpnY>. Acesso em: 29 abr. 2014.

SILVA, Cássia Lopes da. **O direito penal e sistema informático.** São Paulo: Revista dos Tribunais, 2003.

SOUSA, Áurea Maria Ferraz de. **A suspensão condicional do processo pode ser revogado após o período de prova**, jun. 2009. Disponível em: <http://ww3.lfg.com.br/public_html/article.php?story=20090625204108169&mode=print>. Acesso em: 20 maio 2014.

STUMM, Raquel Denise. **Princípio da Proporcionalidade**. Porto Alegre: Livraria do Advogado, 1995.

TANENBAUM, Andrews S. **Redes de computadores.** Tradução Vandenberg D. de Souza. 4. ed. Rio de Janeiro: Elsevier, 2003.

TURBAN, Efraim; McLEAN, Ephraim; WETHERBE, James. **Tecnologia da informação para gestão.** Tradução Renate Schinke. 3. ed. Porto Alegre: Bookman, 2004.

GLOSSÁRIO

ARPANET (Advanced Research Projects Agency): Rede de computadores originada em 1969 pelo Departamento de Defesa norte-americano, conectando instituições militares. Em meados dos anos 70 renomadas universidades americanas aderiram à rede, a qual deu lugar à Internet.

Cracker: Espécie de pirata virtual, que ingressa de forma remota em computadores conectados à Rede com o intuito de causar dano ou obter dados e informações de forma indevida.

Driver: Elemento de *software* que possibilita que o computador se comunique com um acessório específico, como uma determinada placa, por exemplo. Cada tipo de acessório requer um *driver* específico.

E-mail: Comunicação de algum tipo de escrita, com envio e recepção usando computador.

Firewall: Espécie de sistema de segurança que tem por finalidade filtrar o acesso a uma rede. É muito utilizado por empresas, a fim de protegerem as suas redes internas conectadas à Internet contra o acesso de usuários não autorizados.

Hacker: Indivíduo com profundo entendimento sobre o funcionamento de sistemas informáticos, principalmente quando estes estiverem conectados a redes de computadores. O termo tem sido usado equivocadamente como sinônimo de *cracker*.

Hacking: É o ato de hackear sistemas.

Hardware: O equipamento em si, os seus circuitos internos. O equipamento físico ou dispositivos que constituem um sistema informático.

Internetworking: Procedimento de interconexão de redes. Ato de conectar várias redes informatizadas entre si a fim de formar uma só rede de nível mais elevado.

IP (Internet Protocol): Protocolo desenvolvido em meados dos anos 70, o qual permite a comunicação entre computadores, ainda que estes sejam de plataformas diferentes ou estejam distantes.

Ipad: Nome de um *tablet* produzido pela empresa Apple Inc. Possuindo uma tela de 9,7 polegadas e pesando aproximadamente 700 gramas, esta espécie de *tablet* se enquadra entre um *smartphone* e um computador portátil. O Ipad comporta algumas funções de um computador como aplicações, acesso à internet e conteúdos da *Web*, leitor de músicas, vídeos, jogos, etc., sendo utilizado como uma plataforma audiovisual.

Iphone: Linha de *smartphones* fabricados e comercializados pela Apple Inc.

Keylogger: Programa o qual possui a capacidade de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador.

Lan house: Lan significa sigla para Local Area Network, rede de computadores em geral, a qual é limitada a um prédio ou conjunto de prédios de uma instituição. *Lan Houses* são lugares onde se pode acessar a Rede de Internet, como prestação de serviço.

Link: Ligação ou elo. Em ambiente informático pode ser traduzido como a conexão entre um elemento de um documento de hipertexto com outro elemento do documento. O usuário ativa o vínculo dando um clique sobre o elemento vinculado, que é geralmente sublinhado ou apresentado em cor diferente do restante do documento, indicando, desta forma que o elemento encontra-se vinculado.

Login: Entrada em um sistema. Processo pelo qual o usuário se identifica com determinado sistema por meio de senhas, as quais possibilitam acesso aos arquivos e aos demais recursos existentes no sistema.

Log: Registro de atividades formados por programas e serviços de um computador.

Malware: Termo que se refere a todos os tipos de programas que executam ações maliciosas em um sistema informático.

Netbook: Nome utilizado para descrever uma classe de computadores portáteis com dimensão pequena ou média, peso-leve, de baixo custo e que é geralmente utilizado para serviços baseados na internet, como navegação na *Web*.

Notebook: Computador portátil que, em geral, pesa menos que 3 quilos, sendo cabível em uma pasta.

On-line: Expressão que significa ‘estar conectado’. No contexto de um *web site*, significa estar disponível para acesso imediato a uma página de internet, em tempo real. Na comunicação instantânea, significa estar pronto para a transmissão imediata de dados, seja por meio falado ou escrito. No contexto de um outro sistema de informação, significa estar em plena operação, de acordo com as funções desempenhadas nessa rede ou sistema.

Pc: Termo usado para descrever computadores de uso pessoal e doméstico.

Pendrive: Dispositivo móvel para o armazenamento de dados

Phishing scam: Mensagem que induz o usuário à instalação de códigos maliciosos, além da mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros.

Phreakers: Nome dado aos chamados *hackers* em telefonia.

Protocolo de Transferência de Arquivos (FTP): Designa o principal protocolo de transferência de arquivos usados na Internet, ou então um programa que usa esse protocolo.

Um protocolo-padrão da Internet que é usado para transferência de arquivos entre computadores.

Site: Local na internet identificado por um nome de domínio, constituído por uma ou mais páginas de hipertexto, que podem conter textos, gráficos e informações multimídia.

Smarthphone: Espécie de celular com tecnologias avançadas, o qual inclui programas executados em um sistema operacional, equivalente aos computadores.

SMS: Tecnologia amplamente utilizada em telefonia celular para a transmissão de mensagens de texto curtas (cada mensagem é limitada em 160 caracteres alfanuméricos).

Software: Conjunto de programas, procedimentos, regras e documentação relacionados com o funcionamento e manuseio de um sistema de dados.

Spammers: Usuários que enviam *spams.*

Spywares: Categoria de *software* que tem o objetivo de monitorar atividades de um sistema e enviar informações coletadas para terceiros. Podem ser utilizados de forma legítima, mas na maioria das vezes o são de forma dissimulada, não autorizada e maliciosa.

Tablets: Tipo de computador portátil em forma de prancheta, de tamanho pequeno, e com tela sensível ao toque (*touchscreen*). É um dispositivo prático com uso semelhante a um computador portátil convencional, no entanto, é mais destinado para fins de entretenimento que para uso profissional.

Team Viewer: Tradicional programa para acesso remoto. Seu principal objetivo é facilitar o acesso e o compartilhamento de dados entre dois computadores, conectados pela Rede de computadores.

Trojan horse: Programa recebido, normalmente, na forma de um "presente" (cartão virtual, protetor de tela, jogo, etc.), que executa não só as funções para as quais foi aparentemente projetado, mas também outras funções normalmente maliciosas e sem o conhecimento do usuário.

Unidade de Processamento de Dados (CPU): O processador central de um sistema de computador. Contém a memória principal, unidade aritmética e um grupo de registros especiais.

Web: Sistema de informações ligadas através de hipermídia (hiperligações em forma de texto, vídeo, som e outras animações digitais) que possibilita o acesso pelo usuário a uma infinidade de conteúdos através da internet.

ANEXOS

ANEXO A – Lei Ordinária nº 12. 737/2012 – Lei Carolina Dieckmann

LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.

Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2. 848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências.

A PRESIDENTA DA REPÚBLICA

Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

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

Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:

"Invasão de dispositivo informático

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

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

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

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

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

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

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

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

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

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

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

"Ação penal

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

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

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

Art. 266.....

§ 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

§ 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública." (NR)

"Falsificação de documento particular

Art. 298. .....

Falsificação de cartão

Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito." (NR)

Art. 4º Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.

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

DILMA ROUSSEFF

ANEXO B – PL nº 2793/2011 – Proposição Originária

PROJETO DE LEI Nº 2793, DE 2011

Dos Srs. Paulo Teixeira, Luiza Erundina, Manuela D´Àvila, João Arruda, Brizola Neto, Emiliano José

Dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.

O CONGRESSO NACIONAL DECRETA:

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. Devassar 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 autorização expressa ou tácita do titular do dispositivo, instalar vulnerabilidades ou 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 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 e 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.

§ 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, se o fato não constitui crime mais grave.

§ 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 Assembléia Legislativa de Estado; da Câmara Legislativa do Distrito Federal ou de Câmara de Vereadores; 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 artigos 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 entrará em vigor cento e vinte dias após a data de sua publicação.

JUSTIFICAÇÃO

São inegáveis os avanços para a sociedade decorrentes do uso da Internet e das novas tecnologias. Estes avanços trazem a necessidade da regulamentação de aspectos relativos à sociedade da informação, com o intuito de assegurar os direitos dos cidadãos e garantir que a utilização destas tecnologias possa ser potencializada em seus efeitos positivos e minimizada em seus impactos negativos. Nesta discussão, ganha relevo constante, sendo

objeto de amplos debates sociais, a temática da repressão criminal a condutas indesejadas praticadas por estes meios.

Dentre os inúmeros projetos que abordam a matéria, encontra-se em estado avançado de tramitação neste Congresso Nacional um projeto de lei - o PL 84/99, de autoria do Deputado Luiz Piauhylino - que tem por objeto a tipificação de "condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares". Tal projeto, aprovado no Senado Federal em 2008, na forma de um substitutivo, encontra-se em tramitação final nesta Câmara dos Deputados.

A nosso ver, o PL 84/1999, em sua redação atual, traz propostas de criminalização demasiadamente abertas e desproporcionais, capazes de ensejar a tipificação criminal de condutas corriqueiras praticadas por grande parte da população na Internet. Ainda, fixa em um diploma penal matérias - como guarda e acesso a registros de conexão - que deveriam constar de uma regulamentação da Internet que fosse mais abrangente e mais atenta aos direitos e garantias do cidadão. Estas características indesejadas foram amplamente levantadas pela sociedade, por meio de manifestos públicos, movimentos virtuais e abaixo-assinados. Também foram apontadas pelos diversos especialistas que tiveram a oportunidade de apresentar suas contribuições e visões sobre a matéria nos seminários e audiências públicas organizados no âmbito da Comissão de Ciência e Tecnologia, Comunicação e Informática da Câmara dos Deputados.

Ocorre que, em seu atual estágio de tramitação, por conta de questões regimentais, o Projeto de Lei referido não pode mais ser emendado ou alterado. Apresentamos, portanto, nossa proposta alternativa de criação de tipos penais específicos para o ambiente da Internet. Esta redação que apresentamos, e que ainda é passível de aperfeiçoamentos e contribuições - sempre de forma a garantir os direitos do cidadão na Internet e evitar a criminalização de condutas legítimas e corriqueiras na Internet - é resultado, portanto, de um processo amplo de discussão, e que iniciou com a submissão de uma minuta preliminar e tentativa no portal e-Democracia, espaço de debate público e participação social por meios eletrônicos da Câmara dos Deputados.

A proposta, em sua elaboração, contou também com a participação de órgãos do governo e de representantes da sociedade civil.

Nossa proposta observa, ainda, os direitos e garantias do cidadão que utiliza a Internet, nos termos propostos pelo já mencionado PL 2.126/2010, em tramitação nesta Câmara dos Deputados. Em nosso entendimento, a aprovação deste Projeto deve ser precedida da aprovação do Marco Civil da Internet. Não se deve admitir que legislações penais - infelizmente, um mal necessário em nossa sociedade - precedam o estabelecimento de direitos e garantias. A face repressiva do Estado não deve sobressair sobre seu papel como fiador máximo dos direitos do cidadão.

Em sua redação, buscamos evitar incorrer nos mesmos erros do PL 84/1999. O Projeto propõe, sim, a criação de tipos penais aplicáveis à condutas praticadas na Internet mas apenas aquelas estritamente necessárias à repressão daquelas atividades socialmente reconhecidas como ilegítimas e graves.

Vejamos algumas diferenças entre este Projeto e o PL 84/1999.Em primeiro lugar, destaca-se que o presente projeto trata apenas de tipificações penais. Diferentemente do PL 84/99, não se abordam as questões relativas a guarda e fornecimento de registros, ou demais obrigações imputáveis a provedores de serviços de internet - questões que encontram lugar mais adequado numa regulamentação civil sobre a matéria.

Em segundo lugar, cabe notar que a presente proposta apresenta um número de tipos penais significativamente inferior àquele apresentado pelo PL 84/99. Norteamo-nos, nesta escolha, pela compreensão de que grande parte das condutas relativas praticadas por meios eletrônicos já se encontra passível de punição pelo ordenamento jurídico pátrio. Ainda, pautamo-nos pela visão de que não é a proliferação de tipos penais que levará à maior repressão de condutas.

Foram excluídas as definições pretensamente exaustivas do PL original, as quais não significavam ganho em precisão e clareza da legislação penal, dada a natureza muito ampla e indeterminada das respectivas redações. Buscou-se, a este respeito, a utilização de terminologias que já encerrasse de forma adequada as condutas que se pretende criminalizar, sem estendê-las indevidamente.

Ainda, com relação ao PL 84/99, nota-se que grande parte dos tipos penais ali propostos apresenta redação significativamente aberta, e muitas vezes sob a forma de tipos de mera conduta, cuja simples prática - independentemente do resultado obtido ou mesmo da específica caracterização da intenção do agente - já corresponderia à consecução da atividade criminosa.

Tal estratégia redacional, típica de uma sociedade do risco e de uma lógica de direito penal do inimigo, busca uma antecipação da tutela penal a esferas anteriores ao dano, envolvendo a flexibilização das regras de causalidade, a tipificação de condutas tidas como irrelevantes, a ampliação e a desproporcionalidade das penas e a criação de delitos de perigo abstrato, dentre outras características. Exemplo disso é a criação de um capítulo com o objetivo de tutelar juridicamente, como bem jurídico protegido, a “segurança dos sistemas informatizados”. Tal estratégia, como já apontado, resulta na possibilidade de punição gravosa a meras condutas que, por sua natureza ou intenção, não mereceriam ensejar a repressão penal - como o acesso não autorizado a sistemas informáticos decorrentes de testes de segurança efetuados sem a prévia anuência dos titulares de sistemas informatizados.

Em contrapartida a esta tendência, o presente projeto de lei busca equilibrar as penas previstas segundo a gravidade das condutas, hierarquizando, a partir de um tipo principal, os patamares de penas aplicáveis a partir dos resultados danosos obtidos pela prática dos atos tipificados - e, obviamente, buscando harmonizar as penas previstas com as já existentes no ordenamento jurídico brasileiro.

Busca, tanto quanto possível, orientar as tipificações a partir de um fim especial de agir, consistente na intenção consciente do agente em praticar determinada modalidade de atividade danosa a terceiro. Reinsere as condutas tipificadas na lógica atual dos bens jurídicos penalmente tutelados pelo ordenamento, evitando a expansão desnecessária da proteção penal para novas searas. Acrescenta como elementos básicos do tipo critérios de verificação - de modo, de meio, de finalidade - para que se verifique a conduta como efetivamente punível, buscando assim mitigar os efeitos indesejados de uma tipificação demasiadamente aberta sobre condutas sociais corriqueiras.

Passando à análise específica dos tipos propostos, iniciemos pelo tipo de “invasão de dispositivo informático”, proposto como art. 154-A. O tipo insere-se no capítulo referente a crimes contra a liberdade individual, e na seção correspondente aos crimes contra a inviolabilidade de segredos. Apresenta como elemento nuclear o verbo “devassar”, representando assim um acesso indevido, e aproveitando-se da jurisprudência já consolidada a respeito do tema quanto à violação de correspondência.

Determina que o objeto da violação seja o “dispositivo informático alheio, conectado ou não a rede de computadores”. Evita-se, assim, a tipificação dos casos de violação ou devassa de um equipamento do próprio proprietário, como a remoção de medidas técnicas de proteção embutidas em sistemas operacionais de dispositivos informáticos.

Estabelece como elemento necessário para a configuração do crime a violação indevida de mecanismo de segurança - evitando, assim, a criminalização do mero acesso a dispositivos desprotegidos, ou ainda a violação legítima a mecanismos de segurança, como a eliminação de uma medida técnica de proteção que inviabilize o acesso legítimo, em outro dispositivo informático, de uma CD ou DVD protegido, por exemplo.

Por fim, estabelece a necessidade de intenção específica de “instalar vulnerabilidades, obter vantagem ilícita ou obter ou destruir dados ou informações nãoautorizados” - ou seja, pune-se apenas quando a conduta do agente estiver relacionada a determinado resultado danoso ou quando o objetivo do agente for efetivamente censurável e não se confundir com atividades legítimas da Internet,excluindo-se assim, mais uma vez, os casos de mero acesso a informações, ou os casos de obtenção de informações que, por sua natureza, não seriam passíveis de restrição de acesso. Quanto à pena, esta equipara-se à de violação de segredo profissional.

Pena semelhante é atribuída aos casos de produção, oferecimento, distribuição,venda ou difusão de programa de computador com o intuito específico de praticar as condutas definidas no caput. Busca-se, assim, sancionar a produção e difusão de vírus de computador e códigos maliciosos, como aqueles empregados para o roubo de senhas e demais atividades nocivas.

Destaque-se, mais uma vez, a necessidade de que a finalidade específica do agente que produz, oferece, distribui, vende ou difunde tal programa de computador seja a de permitir que terceiros pratiquem as atividades nocivas anteriormente tipificadas. Afasta-se, assim, a tipificação da produção e distribuição de ferramentas que tenham por finalidade o mero teste de segurança de sistemas informáticos - e que, caso empregadas indevidamente, possam servir a finalidades nocivas. Isto porque faz-se necessário ao agente o dolo específico de permitir práticas criminosas.

Estabelecemos, ainda, penas proporcionalmente maiores ou causas de aumento de pena para quando a invasão apresentar resultados concretos revestidos de lesividade ainda maior. Isso ocorre, por exemplo, quando, como consequência da invasão, resulta prejuízo econômico para o proprietário do dispositivo invadido, ou quando da invasão resulta o controle remoto do dispositivo invadido, como nos casos da invasão de computadores de terceiros para a prática de atividades nocivas a partir deles. Também se prevê pena maior - de seis meses a dois anos, e multa - para os casos em que, por meio da invasão, o criminoso obtém mensagens de email de terceiros - que são protegidas pelo direito à privacidade, ou informações expressamente reconhecidas como sigilosas em Lei. A pena cominada pode

ainda ser aumentada se houver maior lesividade à privacidade - como nos casos em que houver divulgação, comercialização ou transmissão a terceiro dos dados ou informações sigilosos obtidos.

Ainda no campo da invasão de dispositivos, a proposta traz, em seu parágrafo quinto, traz causa especial de aumento de pena quando o crime é cometido contra determinados sujeitos passivos que correspondam a altas autoridades públicas, por considerar que essas condutas terão lesividade ainda maior.

Quanto a estes crimes, destaca-se que, quando cometidos contra particular, deverão ser objeto de ação penal pública condicionada à apresentação de representação pelo interessado. Evita-se, assim, que haja repressão a condutas reputadas inofensivas pelos próprios ofendidos, com o consequente desperdício de recursos na ação estatal repressiva.

O projeto traz ainda duas alterações de artigos já existentes no Código Penal.

O primeiro diz respeito à tipificação da conduta de interrupção, impedimento ou dificultação do restabelecimento de serviço telemático ou de serviço de informação de utilidade pública. Trata-se de ampliação do tipo atualmente previsto no art. 266 do Código Penal, que, atualmente, protege apenas os serviços telegráficos, radiotelegráficos ou telefônicos. É, portanto, mera "atualização tecnológica" da redação de dispositivo já existente. A esse respeito, destaque-se que um tipo análogo consta da redação da versão atualmente em tramitação do PL 84/1999. No entanto, no âmbito do PL 84/99, também consta como núcleo do tipo penal a mera "perturbação" de tais serviços, o que poderia abranger condutas inofensivas como o excesso de utilização de determinado serviço.

O PL 84/99 também inseria como bens protegidos os serviços "telemático, informático, de dispositivo de comunicação, de rede de computadores, de sistema informatizado ou de telecomunicação". Destes, foram mantidos apenas o "telemático" e o "de informação de utilidade pública". Assim, foram mantidos aqueles serviços que corresponderiam essencialmente a serviços públicos - uma vez que o tipo penal insere-se no Capítulo que trata "dos crimes contra a segurança dos meios de comunicação e transporte e outros serviços públicos" - e excluídos aqueles cuja natureza, eminentemente privada, não merecesse este nível de equiparação.

Por fim, incluiu-se a equiparação de cartões bancários eletrônicos, de crédito e débito, a documentos particulares, para permitir a tipificação no âmbito do crime de falsificação de documento particular. Trata-se de dispositivo não previsto no PL original e que preenche omissão hoje existente em nosso ordenamento. Dada atipicidade estrita do direito penal, é preciso efetuar tal alteração para deixar claro que o crime de "falsificação" também ocorre quando o objeto é um cartão de crédito ou débito.

Espera-se, com este projeto, oferecer à sociedade uma alternativa equilibrada de repressão a condutas socialmente consideradas como indesejáveis, sem no entanto operar a criminalização excessiva e demasiado aberta que permitiria considerar todo e qualquer cidadão como um potencial criminoso em seu uso cotidiano da rede mundial de computadores.

Conclamo, assim, os nobres Pares para juntos aprovarmos este projeto de lei e aperfeiçoá-lo durante a sua tramitação nesta Casa de Leis.

ANEXO C – Lei Ordinária nº 12. 735/2012 – Lei Azeredo

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 nº1.001, 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.

A PRESIDENTA DA REPÚBLICA

Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º Esta Lei altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.

Art. 2º (VETADO)

Art. 3º (VETADO)

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

Art. 5º O inciso II do § 3º do art. 20 da Lei nº 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação:

> "Art. 20. .....
> .....
>
> § 3º .....
> .....
>
> II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio;
> ....." (NR)

Art. 6º Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.

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

DILMA ROUSSEFF

ANEXO D – PL nº 84/1999 – Proposição Originária

PROJETO DE LEI Nº 84, DE 1999

Do deputado Luiz Piauhylino - PSDB/PE

Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências.

Capítulo I

Dos princípios que regulam a prestação de serviço por redes de computadores

Art. 1º. O acesso, o processamento e a disseminação de informações através das redes de computadores devem estar a serviço do cidadão e da sociedade, respeitados os critérios de garantia dos direitos individuais e coletivos de privacidade e segurança de pessoas físicas e jurídicas e da garantia de acesso às informações disseminadas pelos serviços da rede.

Art. 2º. É livre a estruturação e o funcionamento das redes de computadores e seus serviços, ressalvadas as disposições específicas reguladas em lei.

Capítulo II

Do uso de informações disponíveis em computadores ou redes de computadores

Art. 3º. Para fins desta lei, entende-se por informações privadas aquelas relativas à pessoa física ou jurídica identificada ou identificável.

Parágrafo único. É identificável a pessoa cuja individuação não envolva custos ou prazos desproporcionados.

Art. 4º. Ninguém será obrigado a fornecer informações sobre sua pessoa ou de terceiros, salvo nos casos previstos em lei.

Art. 5º. A coleta, o processamento e a distribuição, com finalidades comerciais, de informações privadas ficam sujeitas à prévia aquiescência da pessoa a que se referem, que poderá ser tornada sem efeito a qualquer momento, ressalvando-se o pagamento de indenizações a terceiros, quando couberem.

§ 1º A toda pessoa cadastrada dar-se-á conhecimento das informações privadas armazenadas e das respectivas fontes.

§ 2º Fica assegurado o direito à retificação de qualquer informação armazenada incompleta.

§ 3º Salvo por disposição legal ou determinação judicial em contrário, nenhuma informação privada será mantida à revelia da pessoa a que se refere ou além do tempo previsto para sua validade.

§ 4º Qualquer pessoa física ou jurídica tem o direito de interpelar o proprietário da rede de computadores ou provedor de serviço para saber se mantém informações a seu respeito, e o respectivo teor.

Art. 6º. Os serviços de informações ou de acesso a bancos de dados não distribuirão informações privadas referentes, direta ou indiretamente, a origem racial, opinião política, filosófica, religiosa ou de orientação sexual e de filiação a qualquer entidade, pública ou privada, salvo autorização expressa do interessado.

Art. 7º. O acesso de terceiros não autorizados pelos respectivos interessados a informações privadas mantidas em redes de computadores dependerá de prévia autorização judicial.

Capítulo III

Seção I

Dano a dado ou programa de computador

Art. 8º. Apagar, destruir, modificar ou de qualquer forma inutilizar, total ou parcialmente, dado ou programa de computador, de forma indevida ou não autorizada.

Pena: detenção, de um a três anos e multa.

Parágrafo único. Se o crime é cometido:

I - contra interesse da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II - com considerável prejuízo para a vítima;

III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV - com abuso de confiança;

V - por motivo fútil;

VI - com uso indevido de senha ou processo de identificação de terceiro;

VII - com a utilização de qualquer outro meio fraudulento.

Pena: detenção, de dois a quatro anos e multa.

Seção II

Acesso indevido ou não autorizado

Art. 9º. Obter acesso indevido ou não autorizado a computador ou rede de computadores.

Pena: detenção, de seis meses a um ano e multa.

§ 1º Na mesma pena incorre quem sem autorização, ou indevidamente, obtém, mantém ou fornece a terceiro qualquer meio de identificação ou acesso a computador ou rede de computadores.

§ 2º Se o crime é cometido:

I - com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II - com considerável prejuízo para a vítima;

III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV - com abuso de confiança;

V - por motivo fútil;

VI - com uso indevido de senha ou processo de identificação de terceiro;

VII - com a utilização de qualquer outro meio fraudulento.

Pena: detenção, de um a dois anos e multa.

Seção III

Alteração de senha ou mecanismo de acesso a programa de computador ou dados

Art. 10. Apagar, destruir, alterar, ou de qualquer forma inutilizar, senha ou qualquer outro mecanismo de acesso a computador, programa de computador ou dados, de forma indevida ou não autorizada.

Pena: detenção, de um a dois anos e multa.

Seção IV

Obtenção indevida ou não autorizada de dado ou instrução de computador

Art. 11. Obter, manter ou fornecer, sem autorização ou indevidamente, dado ou instrução de computador.

Pena: detenção, de três meses a um ano e multa.

Parágrafo único. Se o crime é cometido:

I - com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II - com considerável prejuízo para a vítima;

III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV - com abuso de confiança;

V - por motivo fútil;

VI - com uso indevido de senha ou processo de identificação de terceiro;

VII - com a utilização de qualquer outro meio fraudulento.

Pena: detenção, de um a dois anos e multa.

Seção V

Violação de segredo armazenado em computador, meio magnético, de natureza magnética, óptica ou similar

Art. 12. Obter segredos de indústria ou comércio ou informações pessoais armazenadas em computador, rede de computadores, meio eletrônico de natureza magnética, óptica ou similar, de forma indevida ou não autorizada.

Pena: detenção, de um a três anos e multa.

Seção VI

Criação, desenvolvimento, ou inserção em computador de dados ou programa de computador com fins nocivos

Art. 13. Criar, desenvolver ou inserir dado ou programa em computador ou rede de computadores, de forma indevida ou não autorizada, com a finalidade de apagar, destruir, inutilizar ou modificar dado ou programa de computador ou de qualquer forma dificultar ou impossibilitar, total ou parcialmente, a utilização de computador ou rede de computadores.

Pena: reclusão, de uma a quatro anos e multa.

Parágrafo único**.** Se o crime é cometido:

I - contra interesse da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II - com considerável prejuízo para a vítima;

III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV - com abuso de confiança;

V - por motivo fútil;

VI - com uso indevido de senha ou processo de identificação de terceiro;

VII - com a utilização de qualquer outro meio fraudulento.

Pena: reclusão, de dois a seis anos e multa.

Seção VII

Veiculação de pornografia através da rede de computadores

Art. 14. Oferecer serviço ou informação de caráter pornográfico, em rede de computadores, sem exibir previamente, de forma facilmente visível e destacada, aviso sobre sua natureza, indicando o seu conteúdo e a inadequação para crianças ou adolescentes.

Pena: detenção, de um a três anos e multa.

Capítulo IV

Art. 15. Se qualquer dos crimes previstos nessa lei é praticado no exercício da atividade profissional ou funcional, a pena é aumentada de um sexto até a metade.

Art. 16. Nos crimes definidos nessa lei somente se procede mediante representação do ofendido, salvo se cometidos contra interesse da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta, empresa concessionária de serviços públicos, fundação mantidas ou instituídas pelo poder público, serviços sociais autônomos, instituições financeiras ou empresa que explorem ramo de atividade controlada pelo Poder Público, casos em que a ação é pública incondicionada.

Art. 17. Esta Lei regula os crimes relativos à informática sem prejuízo das demais cominações previstas em outros diplomas legais.

Art. 18. Esta Lei entra em vigor 30 (trinta) dias a contar da data de sua publicação.

SUBSTITUTIVO DO SENADO AO PROJETO DE LEI DA CÂMARA Nº 89, DE 2003 (PL Nº 84, DE 1999)

Substitua-se o Projeto pelo seguinte:

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), a Lei nº 7.716, de 5 de janeiro de 1989, a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 10.446, de 8 de maio de 2002, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.

O CONGRESSO NACIONAL DECRETA:

Art. 1º Esta Lei altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei nº 7.716, de 5 de janeiro de 1989, a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 10.446, de 8 de maio de 2002, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.

Art. 2º O Título VIII da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do Capítulo IV, com a seguinte redação:

"CAPÍTULO IV

DOS CRIMES CONTRA A SEGURANÇA DOS SISTEMAS INFORMATIZADOS

Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado

Art. 285-A. Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.

Obtenção, transferência ou fornecimento não autorizado de dado ou informação

Art. 285-B. Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível:

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.

Ação Penal

Art. 285-C. Nos crimes definidos neste Capítulo somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e subsidiárias."

Art. 3º O Título I da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do seguinte artigo, com a seguinte redação:

"**Divulgação ou utilização indevida de informações e dados pessoais**

Art. 154-A. Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal:

Pena – detenção, de 1 (um) a 2 (dois) anos, e multa.

Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte."

Art. 4º O **caput** do art. 163 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passa a vigorar com a seguinte redação:

"**Dano**

Art. 163. Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio: ....." (NR)

Art. 5º O Capítulo IV do Título II da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do art. 163-A, assim redigido:

"**Inserção ou difusão de código malicioso**

Art. 163-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado:

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Inserção ou difusão de código malicioso seguido de dano

§ 1º Se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado pelo legítimo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado:
Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

§ 2º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte."

Art. 6º O art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passa a vigorar acrescido dos seguintes dispositivos:

"Art. 171. .....
.....

§ 2º Nas mesmas penas incorre quem:
.....

Estelionato Eletrônico

VII – difunde, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado.

§ 3º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime previsto no inciso VII do § 2º, a pena é aumentada de sexta parte." (NR)

Art. 7º Os arts. 265 e 266 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passam a vigorar com as seguintes redações:

"**Atentado contra a segurança de serviço de utilidade pública**

Art. 265. Atentar contra a segurança ou o funcionamento de serviço de água, luz, força, calor, informação ou telecomunicação, ou qualquer outro de utilidade pública:
....." (NR)

"**Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema informatizado**

Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico, telemático, informático, de dispositivo de comunicação, de rede de computadores, de sistema informatizado ou de telecomunicação, assim como impedir ou dificultar-lhe o restabelecimento:
....." (NR)

Art. 8º O **caput** do art. 297 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passa a vigorar com a seguinte redação:

"**Falsificação de dado eletrônico ou documento público**

Art. 297. Falsificar, no todo ou em parte, dado eletrônico ou documento público, ou alterar documento público verdadeiro:
....." (NR)

Art. 9º O **caput** do art. 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passa a vigorar com a seguinte redação:

“**Falsificação de dado eletrônico ou documento particular**

Art. 298. Falsificar, no todo ou em parte, dado eletrônico ou documento particular ou alterar documento particular verdadeiro:
..........” (NR)

Art. 10. O art. 251 do Capítulo IV do Título V da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passa a vigorar acrescido do inciso VI ao seu § 1º, e do § 4º, com a seguinte redação:

“Art. 251. .....

§ 1º Nas mesmas penas incorre quem:
.....

Estelionato Eletrônico

VI - Difunde, por qualquer meio, código malicioso com o intuito de facilitar ou permitir o acesso indevido a rede de computadores, dispositivo de comunicação ou a sistema informatizado, em prejuízo da administração militar.
.....

§ 4º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.” (NR)

Art. 11. O **caput** do art. 259 e o **caput** do art. 262 do Capítulo VII do Título V da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passam a vigorar com a seguinte redação:

“**Dano Simples**

Art. 259. Destruir, inutilizar, deteriorar ou fazer desaparecer coisa alheia ou dado eletrônico alheio, desde que este esteja sob administração militar:
.....” (NR)

“**Dano em material ou aparelhamento de guerra ou dado eletrônico**

Art. 262. Praticar dano em material ou aparelhamento de guerra ou dado eletrônico de utilidade militar, ainda que em construção ou fabricação, ou em efeitos recolhidos a depósito, pertencentes ou não às forças armadas:
.....” (NR)

Art. 12. O Capítulo VII do Título V da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), fica acrescido do art. 262-A, com a seguinte redação:

“**Inserção ou difusão de código malicioso**
Art. 262-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado, desde que o fato atente contra a administração militar:

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Inserção ou difusão de código malicioso seguido de dano

§ 1º Se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento não autorizado pelo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado:

Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

§ 2º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte."

Art. 13. O Título VII da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), fica acrescido do Capítulo VIII, com a seguinte redação:

"CAPÍTULO VIII

DOS CRIMES CONTRA A SEGURANÇA DOS SISTEMAS INFORMATIZADOS

Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado

Art. 339-A. Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, desde que o fato atente contra a administração militar:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.

Obtenção, transferência ou fornecimento não autorizado de dado ou informação

Art. 339-B. Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível, desde que o fato atente contra a administração militar:

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.

Divulgação ou utilização indevida de informações e dados pessoais

Art. 339-C. Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado sob administração militar com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal:

Pena – detenção, de 1 (um) a 2 (dois) anos, e multa.

Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte."

Art. 14. O **caput** do art. 311 do Capítulo V do Título VII do Livro I da Parte Especial do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passa a vigorar com a seguinte redação:

"**Falsificação de documento**

Art. 311. Falsificar, no todo ou em parte, documento público ou particular, ou dado eletrônico ou alterar documento verdadeiro, desde que o fato atente contra a administração ou o serviço militar:
.........." (NR)

Art. 15. Os incisos II e III do art. 356 do Capítulo I do Título I do Livro II da Parte Especial do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passam a vigorar com a seguinte redação:

"CAPÍTULO I

DA TRAIÇÃO

Favor ao inimigo

Art. 356. .....
.....

II - entregando ao inimigo ou expondo a perigo dessa conseqüência navio, aeronave, força ou posição, engenho de guerra motomecanizado, provisões, dado eletrônico ou qualquer outro elemento de ação militar;

III - perdendo, destruindo, inutilizando, deteriorando ou expondo a perigo de perda, destruição, inutilização ou deterioração, navio, aeronave, engenho de guerra motomecanizado, provisões, dado eletrônico ou qualquer outro elemento de ação militar.
.........." (NR)

Art. 16. Para os efeitos penais considera-se, dentre outros:

I – dispositivo de comunicação: qualquer meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia;

II – sistema informatizado: qualquer sistema capaz de processar, capturar,
armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente;

III – rede de computadores: o conjunto de computadores, dispositivos de comunicação e sistemas informatizados, que obedecem a um conjunto de regras, parâmetros, códigos, formatos e outras informações agrupadas em protocolos, em nível topológico local, regional, nacional ou mundial através dos quais é possível trocar dados e informações;

IV – código malicioso: o conjunto de instruções e tabelas de informações ou qualquer outro sistema desenvolvido para executar ações danosas ou obter dados ou informações de forma indevida;

V – dados informáticos: qualquer representação de fatos, de informações ou de conceitos sob forma suscetível de processamento numa rede de computadores ou dispositivo de comunicação ou sistema informatizado;

VI – dados de tráfego: todos os dados informáticos relacionados com sua comunicação efetuada por meio de uma rede de computadores, sistema informatizado ou dispositivo de comunicação, gerados por eles como elemento de uma cadeia de comunicação, indicando origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.

Art. 17. Para efeitos penais consideram-se também como bens protegidos o dado, o dispositivo de comunicação, a rede de computadores, o sistema informatizado.

Art. 18. Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

Art. 19. O inciso II do § 3º do art. 20 da Lei nº 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação:

"Art. 20 .....
.....

§ 3º.....
.....

II – a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas, ou da publicação por qualquer meio.
....." (NR)

Art. 20. O **caput** do art. 241 da Lei nº 8.069, de 13 de julho de 1990, passa a vigorar com a seguinte redação:

"Art. 241. Apresentar, produzir, vender, receptar, fornecer, divulgar, publicar ou armazenar consigo, por qualquer meio de comunicação, inclusive rede mundial de computadores ou Internet, fotografias, imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente:
....." (NR)

Art. 21. O art. 1º da Lei nº 10.446, de 8 de maio de 2002, passa a vigorar com a seguinte redação:

"**Art. 1º** .....
.....

V – os delitos praticados contra ou mediante rede de computadores, dispositivo de comunicação ou sistema informatizado.
....." (NR)

Art. 22. O responsável pelo provimento de acesso a rede de computadores mundial, comercial ou do setor público é obrigado a:

I – manter em ambiente controlado e de segurança, pelo prazo de 3 (três) anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial;

II – preservar imediatamente, após requisição judicial, outras informações requisitadas em curso de investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade;

III – informar, de maneira sigilosa, à autoridade competente, denúncia que tenha recebido e que contenha indícios da prática de crime sujeito a acionamento penal público incondicionado, cuja perpetração haja ocorrido no âmbito da rede de computadores sob sua responsabilidade.

§ 1º Os dados de que cuida o inciso I deste artigo, as condições de segurança de sua guarda, a auditoria à qual serão submetidos e a autoridade competente responsável pela auditoria, serão definidos nos termos de regulamento.

§ 2º O responsável citado no **caput** deste artigo, independentemente do ressarcimento por perdas e danos ao lesado, estará sujeito ao pagamento de multa variável de R$ 2.000,00 (dois mil reais) a R$ 100.000,00 (cem mil reais) a cada requisição, aplicada em dobro em caso de reincidência, que será imposta pela autoridade judicial desatendida, considerando-se a natureza, a gravidade e o prejuízo resultante da infração, assegurada a oportunidade de ampla defesa e contraditório.

§ 3º Os recursos financeiros resultantes do recolhimento das multas estabelecidas neste artigo serão destinados ao Fundo Nacional de Segurança Pública, de que trata a Lei nº 10.201, de 14 de fevereiro de 2001.

Art. 23. Esta Lei entra em vigor 120 (cento e vinte) dias após a data de sua publicação.

Senado Federal, em de julho de 2008

ANEXO E – PL nº 5485/2013 – Proposição Originária

PROJETO DE LEI Nº 5485, DE 2013

Do Sr. Eduardo Azeredo

Dispõe sobre a tipificação criminal do estelionato informático.

O CONGRESSO NACIONAL DECRETA:

Art. 1º Esta Lei dispõe sobre a tipificação criminal do estelionato informático.

Art. 2º O artigo 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passa a vigorar acrescido do inciso VII, com a seguinte redação:

"Estelionato informático

Art. 171.....

§2º Nas mesmas penas incorre quem
.....

VII – envia mensagens digitais de qualquer espécie, fazendo-se passar por empresas, instituições ou pessoas a fim de induzir outrem a revelar informações pessoais, de identidade, ou senhas de acesso."(NR)

Art.3º. Esta lei entra em vigor na data de sua publicação.

JUSTIFICAÇÃO

A imprensa publica quase que diariamente reportagens sobre cidadãos que foram vítimas de invasão em suas contas correntes e cartões de crédito, e a história é sempre a mesma: a pessoa abre sua caixa de correio eletrônico ou sua conta nas redes sociais ou recebe um texto do tipo SMS e encontra uma mensagem aparentemente enviada pelo seu banco pedindo para atualizar suas informações.

Ato contínuo, a pessoa clica no link, é enviada para um website falso – que simula o site do banco original – onde a vítima fornece seus dados pessoais, números de conta e de cartões de crédito e códigos de acesso.

Muitas pessoas não desconfiam que se trate de um golpe e, portanto terão seu dinheiro transferido para outras contas, seus cartões de crédito usados para compras na Internet e terá suas contas de e-mail e de redes sociais invadidas, causando prejuízos e transtornos.

Esse tipo de crime é conhecido na Internet como “phishing”, sendo um golpe comum, e configurado como a forma moderna de engenharia social, ou o estelionato no mundo informático.

A prática do estelionato informático se consubstancia no envio, com intenções fraudulentas, de e-mails que pretendem ser de empresas conceituadas, a fim de induzir as pessoas a revelar informações pessoais, como senhas e/ou números de cartão de crédito.

Essa conduta é usada para o roubo de identidade on-line, utilizando engenharia social e subterfúgios técnicos para obter, de forma indevida e fraudulenta, os dados pessoais, de identidade e as credenciais financeiras dos consumidores.

A prática de phishing, ou estelionato informático, encontra-se em expansão no Brasil, pois existe falta de informação e de campanhas esclarecedoras na imprensa sobre esse tipo de ataque cibernético.

Pior: a maioria dos usuários de Internet não tem conhecimento que seus dados pessoais são alvo constante e valioso de criminosos digitais, e, portanto, não adotam as precauções necessárias em sua conduta on-line.

Além disso, as pessoas que praticam esse tipo de conduta estão adotando tecnologias digitais avançadas para possibilitar a obtenção de dados até mesmo de pessoas que estão cientes e adotam cuidados básicos contra a prática do phishing (estelionato informático).

Essas novas tecnologias se valem de vulnerabilidades dos navegadores de Internet que permitem o download e a execução de programas de computador hospedados em websites hostis.

Sendo assim, fica evidente a necessidade de uma atualização do Código Penal Brasileiro que venha a estabelecer uma tipificação penal relativa ao phishing, ou estelionato informático, de forma a desencorajar esse tipo de prática.

Uma disposição dessa natureza não foi estabelecida nas recentes legislações editadas sobre o assunto - Lei nº 12.737, de 2012 – conhecida como Lei Carolina Dieckmann, e Lei nº 12.735, de 2012.

Este Projeto de Lei, portanto, introduz no Código Penal uma tipificação penal específica que tipifica como crime a prática de difusão de mensagens eletrônicas com o intuito de obter dados pessoais, números de cartão de crédito, senhas, usuários de acesso, de forma fraudulenta.

Essa tipificação tem o objetivo de reduzir a ocorrência desse tipo cada vez mais frequente de golpe na Internet e que causa enormes prejuízos para os consumidores e cidadãos. Além disso, estabelece novos instrumentos legais que poderão ser usados pelos órgãos policiais para ampliar a segurança no domínio brasileiro da Internet.

Diante do exposto, peço o apoio dos nobres Parlamentares desta Casa para a aprovação deste Projeto de Lei.

ANEXO F – PL nº 5555/2013 – Proposição Originária

PROJETO DE LEI Nº 5555, DE 2013

Do Sr. João Arruda

Altera a Lei nº 11.340, de 7 de agosto de 2006 – Lei Maria da Penha – criando mecanismos para o combate a condutas ofensivas contra a mulher na Internet ou em outros meios de propagação da informação.

O CONGRESSO NACIONAL DECRETA:

Art. 1º Esta Lei altera a Lei nº 11.340, de 7 de agosto de 2006 – Lei Maria da Penha – criando mecanismos para o combate a condutas ofensivas contra a mulher na Internet ou em outros meios de propagação da informação.

Art. 2º O artigo 3º da Lei nº 11.340, de 7 de agosto de 2006, passa a vigorar com a seguinte redação:

"Art. 3º Serão asseguradas às mulheres as condições para o exercício efetivo dos direitos à vida, à segurança, à saúde, à alimentação, à educação, à cultura, à comunicação, à moradia, ao acesso à justiça, ao esporte, ao lazer, ao trabalho, à cidadania, à liberdade, à dignidade, ao respeito e à convivência familiar e comunitária." (NR)

Art. 3º O artigo 7º da Lei nº 11.340, de 7 de agosto de 2006, passa a vigorar acrescido do inciso VI, com a seguinte redação:

"Art. 7º.....

VI – violação da sua intimidade, entendida como a divulgação por meio da Internet, ou em qualquer outro meio de propagação da informação, sem o seu expresso consentimento, de imagens, informações, dados pessoais, vídeos, áudios, montagens ou fotocomposições da mulher, obtidos no âmbito de relações domésticas, de coabitação ou de hospitalidade."(NR)

Art. 4º O artigo 22 da Lei nº 11.340, de 7 de agosto de 2006, passa a vigorar acrescido do parágrafo 5º, com a seguinte redação:

"Art.22.....

§5º Na hipótese de aplicação do inciso VI do artigo 7º desta Lei, o juiz ordenará ao provedor de serviço de e-mail, perfil de rede social, de hospedagem de site, de hospedagem de blog, de telefonia móvel ou qualquer outro prestador do serviço de propagação de informação, que remova, no prazo de 24 (vinte e quatro) horas, o conteúdo que viola a intimidade da mulher.(NR)"

Art. 5º Esta Lei entra em vigor na data de sua publicação.

JUSTIFICAÇÃO

A aprovação da Lei nº 11.340, de 7 de agosto de 2006 – Lei Maria da Penha – representa um marco nas políticas públicas de combate à violência física, psicológica, sexual e moral contra as mulheres em ambiente familiar.

Com foco em aspectos de natureza processual penal e em garantias civis, a Lei Maria da Penha reuniu condições para que um único juiz pudesse aplicar todas as medidas pertinentes sobre os casos de violência doméstica contra a mulher, resultando em um ganho inestimável de agilidade nesses processos.

Além disso, os dados de monitoramento e as estatísticas oficiais evidenciam que a ocorrência e, sobretudo, a recorrência das condutas de violência doméstica contra a mulher estão em franco processo de redução.

Entretanto, há uma dimensão da violência doméstica contra a mulher que ainda não foi abordada por nenhuma política pública ou legislação, que é a violação da intimidade da mulher na forma da divulgação na Internet de vídeos, áudios, imagens, dados e informações pessoais da mulher sem o seu expresso consentimento.

Essa conduta é praticada por cônjuges ou ex-cônjuges que se valem da condição de coabitação ou de hospitalidade para obter tais registros, divulgando-os em redes sociais como forma de constrangimento à mulher. Esse tipo de violência se torna progressivamente mais danoso quanto mais disseminado e universalizado, do ponto de vista social e geográfico, está o acesso à Internet no Brasil.

Sendo assim, estamos propondo alterações na Lei Maria da Penha com o intuito de estabelecer a violação da intimidade da mulher como forma de violência doméstica e familiar, o que permitirá que se aplique todo o arcabouço processual e civil do marco legal já instituído também nesse tipo de conduta.

Além disso, incluímos o direito à comunicação no rol dos direitos relacionados na referida lei, visto que o acesso à comunicação sem restrições é condição fundamental para a equalização dos direitos das mulheres no Brasil.

Diante do exposto, peço o apoio dos nobres parlamentares desta Casa para a sua aprovação.

ANEXO G – PL nº 6630/2013 – Proposição Originária

PROJETO DE LEI Nº 6630, DE 2013

Do Sr. ROMÁRIO

Acrescenta artigo ao Código Penal, tipificando a conduta de divulgar fotos ou vídeos com cena de nudez ou ato sexual sem autorização da vítima e dá outras providências.

O CONGRESSO NACIONAL DECRETA:

Art. 1º Esta lei torna crime a conduta de divulgar fotos ou vídeos com cena de nudez ou ato sexual sem autorização da vítima.

Art. 2º O Decreto-lei nº 2848, de 7 de dezembro de 1940, passa a vigorar acrescido do seguinte art. 216-B:

"Divulgação indevida de material íntimo

Art. 216-B. Divulgar, por qualquer meio, fotografia, imagem, som, vídeo ou qualquer outro material, contendo cena de nudez, ato sexual ou obsceno sem autorização da vítima.
Pena – detenção, de um a três anos, e multa.

§1º Está sujeito à mesma pena quem realiza montagens ou qualquer artifício com imagens de pessoas.

§2º A pena é aumentada de um terço se o crime é cometido:

I - com o fim de vingança ou humilhação;

II – por agente que era cônjuge, companheiro, noivo, namorado ou manteve relacionamento amoroso com a vítima com ou sem habitualidade;

§3º A pena é aumentada da metade se o crime é cometido contra vítima menor de 18 (dezoito) anos ou pessoa com deficiência." (NR)

Art. 3º O agente fica sujeito a indenizar a vítima por todas as despesas decorrentes de mudança de domicílio, de instituição de ensino, tratamentos médicos e psicológicos e perda de emprego.

Art. 4º O pagamento da indenização prevista no artigo anterior não exclui o direito da vítima de pleitear a reparação civil por outras perdas e danos materiais e morais.

Art. 5º Se o crime foi cometido por meio da Internet, na sentença penal condenatória, o juiz deverá aplicar também pena impeditiva de acesso às redes sociais ou de serviços de e-mails e mensagens eletrônicas pelo prazo de até dois anos, de acordo com a gravidade da conduta.

Art. 6º Esta Lei entra em vigor na data de sua publicação.

JUSTIFICAÇÃO

A Constituição Federal, que completou 25 anos, já assegura o direito à inviolabilidade da intimidade, vida privada, honra e imagem das pessoas, contudo, lamentavelmente cresce o número de mulheres que tem suas imagens íntimas disponibilizadas, nos meios eletrônicos, por seus ex-companheiros por ato de vingança , humilhação ou autopromoção.

Conforme matéria da Folha de São Paulo, veiculada em 02/10/2013, a divulgação de materiais íntimos é um problema crescente na era das redes sociais, quando imagens que eram privadas durante um relacionamento podem alcançar centenas de sites em pouquíssimo tempo. Por causa dessas condutas, as vítimas têm suas vidas destruídas pela ação de outra pessoa em quem confiavam.

Normalmente, os casos de fotos e vídeos íntimos publicados na rede são provocados por parceiros que não aceitam o fim do relacionamento e que procuram essa forma para atingir a integridade física, moral e psicológica da vítima, esta prática ganhou até um nome: Pornografia da vingança.

Conforme o presidente da Comissão de Tecnologia da Informação da Ordem dos Advogados (OAB) Nacional, Alexandre Rodrigues Atheniense, os crimes de internet estão aumentando porque os autores acreditam que suas ações ficarão impunes. "O desconhecimento da existência de leis e métodos que podem efetivamente punir os infratores também é fator predominante", analisou, acrescentando que as mulheres são as maiores vítimas de crimes virtuais contra a honra.

Analisando a legislação vigente, especificamente o Código Penal, não encontramos, a princípio, uma norma penal específica que defina a conduta de divulgação indevida de material íntimo. As autoridades acabam enquadrando como difamação ou injúria, que possuem pena branda para a gravidade da conduta.

Considerando o mérito e o alcance social da iniciativa, contamos com o apoio dos nossos Pares para sua aprovação.