O PROBLEMA DA TIPIFICAÇÃO DOS CRIMES INFORMÁTICOS: ASPECTOS CONTROVERSOS A RESPEITO DA APLICAÇÃO DO ARTIGO 154-A DA LEI Nº 12.737/2012 "LEI CAROLINA DIECKMANN"

THE PROBLEM OF THE COMPUTER CRIMES CRIMINALIZATION: CONTROVERSIAL ISSUES CONCERNING THE APPLICATION OF ARTICLE 154-A OF LAW Nº 12.737/2012 "CAROLINA DIECKMANN LAW"

ALESSANDRA MARA DE FREITAS SILVA [1]

CRISTIAN KIEFER DA SILVA [2]

RESUMO

No atual contexto da era digital, estamos vivendo uma fase de total disseminação das novas tecnologias, onde os meios de comunicação têm encurtado as distâncias entre os diversos cidadãos de diferentes culturas no mundo. Em detrimento a isso, surge um novo ramo do direito após o advento da internet, proveniente das inúmeras relações jurídicas advindas do ambiente digital. Todavia, o cometimento de crimes informáticos tornou-se bastante comum e diversificado desde então, não sendo acompanhado, porém, pela legislação Penal brasileira, bastante escassa nesse sentido. Os legisladores a cada dia demonstram extrema preocupação com a necessidade de se adequar as normas a esta nova realidade. Muitas vezes são influenciados pela mídia, e editam leis sem a devida preocupação com o conteúdo técnico que

[1] **Mestre em Instituições Sociais, Direito e Democracia pela Universidade FUMEC. Graduada em Direito pela Faculdades Milton Campos. MBA em Gestão Empresarial pela Fundação Getúlio Vargas e LLM em Direito Empresarial pela Fundação Getúlio Vargas. Professora de Direito Administrativo e Prática. Coordenadora do Curso de Direito do Centro Universitário UNA Belo Horizonte/Contagem. Professora de Direito Administrativo do Curso MERITUS ON LINE. Advogada Associada no Escritório de Advocacia Ananias Junqueira Ferraz e Relatora da Comissão de Ética da Ordem dos Advogados do Brasil. Tem experiência na área de Ciência Política, com ênfase em Direito Constitucional e Direito Administrativo.**

[2] **Doutorando em Direito pela Pontifícia Universidade Católica de Minas Gerais. Mestre em Direito pela Pontifícia Universidade Católica de Minas Gerais. Especialista em Processo Civil Aplicado pelo CEAJUFE/IEJA. Bacharel em Administração pela Pontifícia Universidade Católica de Minas Gerais. Bacharel em Direito pela Universidade José do Rosário Vellano. Professor Assistente e Pesquisador em Direito da Faculdade Mineira de Direito da Pontifícia Universidade Católica de Minas Gerais. Professor Auxiliar e Pesquisador em Direito da Escola de Direito do Centro Universitário Newton Paiva. Professor Assistente e Pesquisador em Direito do Centro Universitário UNA. Professor Adjunto e Pesquisador em Direito da Faculdade de Minas (FAMINAS-BH). Membro associado do Conselho Nacional de Pesquisa e Pós-Graduação em Direito (CONPEDI). Membro da Associação Brasileira de Sociologia do Direito e Filosofia do Direito (ABRAFI). Integrante dos Grupos de Pesquisas: Direito, Constituição e Processo "Professor Doutor José Alfredo de Oliveira Baracho Júnior" e Direito, Sociedade e Modernidade "Professora Doutora Rita de Cássia Fazzi".**

estas envolvem. Nesse sentido, o presente trabalho irá abordar os aspectos controversos e as possíveis consequências jurídicas acerca da redação dada pelo artigo 154-A da Lei nº 12.737 de 2012, que dispõe sobre os crimes de invasão de dispositivos informáticos, recebendo o epíteto de “Lei Carolina Dieckmann”.

PALAVRAS-CHAVE: LEI CAROLINA DIECKMAN; ASPECTOS CONTROVERSOS; CRIMES INFORMÁTICOS.

ABSTRACT

In the current context of the digital age, we are experiencing a stage full spread of new technologies, where the media have shortened the distances between different citizens of different cultures in the world. At the expense of this, a new branch of law arises after the advent of the internet, many stemming from the legal relations of the digital environment. However, the commission of computer crimes has become quite common and diversified since then, however, not been accompanied by Brazilian law Criminal, very scarce in this direction. Legislators every day demonstrate extreme concern with the need to adapt the rules to this new reality. Are often influenced by the media, and edit laws without due concern for the technical content of these involve. In this sense, this paper will address the controversial aspects and the possible legal consequences regarding the wording of Article 154-A of Law No. 12,737, 2012, which provides for the crimes of invasion of computing devices, receiving the epithet "Carolina Dieckmann Law".

KEYWORD: CAROLINA DIECKMANN LAW; CONTROVERSIAL ASPECTS; COMPUTER CRIMES.

1 INTRODUÇÃO

A internet, desde a sua existência, tem contribuído para o desenvolvimento da sociedade através, sobretudo, do rompimento de barreiras - da informação, da distância, do conhecimento, de pré-conceitos, das relações afetivas, inclusive - a passos largos. Concomitantemente a essa mudança, a internet é utilizada para a prática de atos ilícitos. É nesse contexto que o presente trabalho procura abordar alguns pontos do novíssimo ramo do Direito - o direito de informática - surgido a partir da necessidade de regulamentar as relações virtuais.

A internet surgiu na década de 60, a partir de pesquisas militares dos EUA em meio à guerra fria com a extinta Rússia. Desde então, este sistema vem se expandindo de uma forma assustadora, tornando-se cada vez mais presente na vida das pessoas ao redor do mundo.

Como ferramenta poderosíssima, a internet é utilizada para as mais variadas finalidades, tais como comunicação, compartilhamento de informações, dados, pesquisas científicas e até mesmo relações afetivas.

Como se pode observar, a dimensão criminal ora verificada na internet não apenas conserva os aspectos tradicionalmente preconizados pelo Direito Penal, como traz à tona peculiaridades desse novo contexto. Assim, condutas igualmente lesivas, mas ainda não-consideradas crimes, por dependerem de regulamentação específica, como é o caso do dano praticado contra informações e programas contidos em computador, proliferam em ritmo acelerado, e por vezes incontrolável.

As mudanças paradigmáticas que estão ocorrendo na sociedade pós-moderna em muito se devem a globalização e a disseminação do computador e da internet. Esta, por estar em um ambiente virtual tem sido palco de inúmeras condutas danosas. O controle destas condutas tem sido tema de discussão no Direito Penal, residindo as principais divergências na necessidade de legislação específica e nas dificuldades de resposta do Estado à tais atos. Analisando os conceitos para essa nova forma de criminalidade, bem como a tipicidade das condutas mais comuns no ciberespaço e refletindo sobre aspectos penais como a teoria do tipo, se faz a crítica da necessidade de tutela penal de novos bens jurídicos, relacionados à Internet, em face de um Estado de intervenção mínima.

Além disso, é relevante observar que o ordenamento jurídico brasileiro é iniciante na seara do direito digital. Os juristas ainda não estão completamente aptos para enfrentar a nova realidade cibernética. Ressalte-se que as dificuldades de identificação e controle de usuários, as controvérsias e discussões sobre a produção de provas baseadas em fontes informacionais, dentre tantos outros, são fatores que estabelecem amplas barreiras no combate a esses crimes. Assim, com finalidade de que haja efetiva aplicação da norma faz-se necessário estudo meticuloso do texto legal regimentar, bem como aquisição de conhecimentos de informática pelos profissionais da área, vez que as informações disseminadas pela internet fluem num tempo muito mais célere do que a lei pelos órgãos envolvidos nesse combate.

Dentre as tantas possibilidades que este novo sistema possibilita, a comunicação entre as pessoas é a mais difundida, ocorrendo pelos mais diversificados meios e através dos mais variados dispositivos, como computadores pessoais, notebooks, smartphones, etc. Graças a essas novas tecnologias digitais e sua grande capacidade de armazenar informações e dados em suas memórias, o mundo expandiu seus horizontes e suas crenças na globalização informacional.

Diante dessa nova realidade cibernética, formou-se também um ambiente bastante propício para o cometimento de diversos tipos de crimes, que em sua grande maioria restavam impunes, haja vista a escassa legislação pertinente sobre o assunto. Após várias tentativas anteriores de se legislar sobre o assunto, em 30 de novembro de 2012, foi promulgada a Lei nº 12.737 de 2012, na tentativa de coibir os abusos cometidos através dos sistemas informáticos, sendo tal lei criada para punir seus responsáveis.

Sob o foco do Direito Penal, será abordado no presente trabalho uma visão bem originária dos principais aspectos dos chamados cibercrimes ou crimes de informática, as condutas classificadas como crimes próprios e impróprios de informática, a figura do criminoso digital, bem como os pontos controvertidos da referida lei.

2 BREVE REFLEXÃO HISTÓRICA SOBRE OS SISTEMAS INFORMACIONAIS

Os termos informática, telemática, bytes, internet, estão cada vez mais presentes no vocabulário e no cotidiano de grande parte da população; o convívio da sociedade com as tecnologias da informação está hoje cada vez mais constante em vários seguimentos da sociedade. Nesse sentido, haja vista o atual contexto, o computador e a internet são indispensáveis ao nosso cotidiano, pois os utilizamos para vários fins, como o lazer, comunicação, trabalho, etc. Até mesmo a Administração Pública utiliza largamente a internet para os mais variados fins.

Se atualmente é difícil imaginar a vida sem a informática, até há pouco tempo, a realidade era outra. Para que possamos entender a magnitude desse instrumento que revolucionou o mundo e o modo com que a utilizamos, se faz necessário que saibamos sua origem.

Primeiramente o que conhecemos por “computador”, vem do latim *computatore*, significando “aquele que calcula, ou faz cômputos”. A história do computador remonta aos povos primitivos da Grécia e Egito, que contavam seus animais com o auxílio de pedras. Posteriormente veio a numeração decimal que conhecemos hoje. Em 2500 a.C., existia uma versão primitiva do ábaco, um dispositivo mecânico que os comerciantes egípcios e romanos utilizavam para computar suas transações e consistia em pequenas pedras presas numa haste ou barbante.

Após isso, vieram as máquinas mecânicas para calcular, como “os bastões de Naiper” criados por John Naiper, inventor dos logaritmos em 1614 e os círculos de proporção, criados por Wiliam Oughtred em 1633, baseados nos logaritmos de Naiper. A primeira calculadora da história foi criada pelo francês Blaise Pascal, que em 1642 somava e subtraia números de oito algarismos. Tal invento inspirou o alemão Gottfried Wilhelm Von Leibniz a aperfeiçoá-la, adicionando a multiplicação e a divisão à máquina (CIVITA, 1986, p. 3).

No final da década de 1930, por conta da segunda guerra mundial, devido ao grande número de projetos simultâneos, a necessidade de mais cálculos aumentou consideravelmente, surgindo assim os computadores com relés eletromecânicos, assim chamados de “Bell a relé”. Não obstante, o primeiro computador eletrônico de grande porte, financiado pelo *Ballistic Research Laboratorry* nos EUA, foi desenvolvido entre 1943-1946 para uso militar, onde seus cálculos previam a da trajetória dos projéteis das armas, chamado de ENIAC “*Electronic Numeric Integrator and Calculator*”, que utilizava 1.500 relés, além de 17.468 válvulas eletrônicas e pesava cerca de trinta toneladas. De 1946 a 1948 foram desenvolvidos os computadores comerciais construídos fora das faculdades, considerados da primeira geração como o Univac ou “*Universal Automatic Computer*”, que teve como primeiro cliente o Departamento de Censo dos EUA, posteriormente, empresas como a *Internacional Business Machine* ou IBM e a Siemens lançaram suas máquinas.

A segunda geração de computadores surgiu com a invenção dos transistores, criados nos laboratórios Bell da ATT em 1948, que substituíram as antigas válvulas, pois eram cem vezes mais rápidos e confiáveis que estas. A terceira geração de computadores surgiu com uma inovação tecnológica que mudou radicalmente os computadores: a criação do circuito integrado ou CI, que consiste na união de vários transistores em uma única peça ou Chip, que possibilitou também a criação dos processadores, unindo vários circuitos integrados em uma única pastilha, o que resultou numa grande redução nas dimensões dos computadores.

Em 1976, Stephen Wozniak e Steven Paul Jobs criaram o Apple I, um microcomputador que revolucionou e mudou para sempre a história da informática no mundo. Em 1981 os grandes fabricantes entraram nessa disputa pelo mercado de computadores pessoais e os tornaram uma realidade, tais como os que temos hoje. Desde a criação do ENIAC, o primeiro computador coletivo e o Apple I, o primeiro computador pessoal, passaram-se apenas trinta anos. Hoje, decorridos cerca de cinquenta anos da apresentação do primeiro computador, as mudanças e evoluções não se contam mais em anos, e sim em meses.

3 INTERNET: UM CAMINHO SEM VOLTA

A internet, de acordo com a lição de Fabrizio Rosa, "consiste num conjunto de tecnologias para acesso, distribuição e disseminação de informação em redes de computadores" (ROSA, 2002). Acrescenta-se que não só a informação é disseminada por essa rede, mas também entretenimento, comunicação, relações jurídicas, comerciais, afetivas, dentre outras, comuns a todos os seres humanos.

Segundo Patrícia Peck Pinheiro, "a internet é mais um meio de comunicação eletrônica, formada não apenas por uma rede mundial de computadores, mas, principalmente, por uma rede mundial de indivíduos" (PINHEIRO, 2008).

Sem dúvida, a internet é um grande avanço tecnológico, mas muito mais que isso, ela se caracteriza pela diminuição do espaço. Apresenta-se como um rompimento de fronteiras, onde possibilita uma democratização das informações e do conhecimento, tudo isso sem que se perca a autonomia das identidades. Com efeito, se de um lado a globalização se manifesta tão favoravelmente através da internet, lado outro a rede se torna um moderno e eficaz ambiente para o cometimento dos mais variados tipos de ilícitos.

De acordo com Carla Rodrigues, a internet "é uma grande rede de comunicação mundial, onde estão interligados milhões de computadores, sejam eles universitários, militares, comerciais, científicos ou pessoais, todos interconectados" (RODRIGUES, 2003, p.3). Ela teve como marco inicial, o contexto da Guerra Fria, época em que havia grande disputa entre os EUA e a União Soviética sobre estratégias tecnológicas e científicas de combate. Conforme leciona Fabrizio Rosa, em 1957, quatro meses após a União Soviética por em órbita o primeiro satélite espacial, (o Sputnik), os Estados Unidos da América anunciavam a criação de uma agência federal norte-americana cujo objetivo era pesquisar e desenvolver alta tecnologia para as forças armadas. (ROSA, 2006, p. 31).

Essa agência, denominada Arpa, *Advance Research Projects Agency,* foi criada com o intuito de manter a rede ativa caso os EUA sofresse um ataque de bombardeios, pois não haveria uma central específica que pudesse ser alvo do mesmo; dessa forma, as informações poderiam transitar por caminhos alternativos, chegando ao seu destinatário.

Nos anos 70, a internet passou a ser utilizada para fins acadêmicos e científicos, e o correio eletrônico a aplicação mais utilizada da rede, foi criado em 1972 por Ray Tomlinson. Já em 1973, a Inglaterra e a Noruega foram ligadas à rede, tornando-se, com isso, um

fenômeno mundial. Em meados da década de 80, o governo estadunidense abriu a rede às empresas e continuou financiando a ARPANET até o ano de 1989, quando também foi lançado o primeiro browser (*Windows*); tendo sido apresentado em Genebra a *World Wide Web* (ROSA, 2002).

Ainda de acordo com o referido autor, devido ao rápido crescimento da ARPANET, Vinton Cerf e Bob Kahn propuseram o *transmission Control Protocol/Internet Protoco*l - TCP/IP, sistema que utilizava uma arquitetura de comunicação em camadas, com protocolos distintos, cuidando de tarefas distintas, onde o TCP, cabia quebrar mensagens em pacotes de um lado e recompô-las de outro e ao IP, cabia descobrir o caminho adequado entre o remetente e o destinatário e enviá-los. (ROSA, 2006, p. 32).

Contudo, em 1989 foi lançado o primeiro browser e a tão conhecida atualmente WWW, ou *World Wide Web* e em 1990 o acesso à internet foi liberada ao grande público, através do primeiro provedor de acessos comercial do mundo, o World, possibilitando que usuários comuns, com seus microcomputadores e um modem tivessem acesso a grande rede mundial de computadores. No mesmo ano, Brasil e Argentina conectaram-se à rede.

4 DIREITO DIGITAL: UM NOVO DESAFIO PARA O MILÊNIO

É importante fazer uma pequena abordagem a respeito do chamado Direito Digital. Ele se constitui como sendo o conjunto de aspectos jurídicos que envolvem a internet. Esse novíssimo ramo do Direito se faz presente a partir da necessidade de regular as diversas relações que envolvem a aplicação da informática. Nesse sentido, a Informática Jurídica se divide em dois ramos diferentes, conforme elenca Fabrízio Rosa: o Direito Civil da Informática e o Direito Penal da Informática (ROSA, 2002).

O avanço assustador da tecnologia e especialmente da área de informática, como dito alhures, anda afetando cada vez mais as relações sociais e por consequência, transformando o cotidiano na vida moderna. Nesse contexto, as inovações tecnológicas vão incidir diretamente no Direito, relações que decorrem dos mais variados tipos de operações relacionadas ao comércio, conhecido também como *e-commerce*, tais como a compra, venda, troca, leilões, propaganda, além de serviços como os dos profissionais liberais e os financeiros e uma infinidade de outras relações comerciais.

Um ramo comercial que está constantemente sob ataque na rede, são os Direitos Autorais, onde a pirataria viola os mais variados tipos de propriedade intelectual. Um deles, os softwares, teve proteção pela Lei nº 59.609/98. Outro ramo que sofreu os impactos da evolução tecnológica foi a área bancária, que utiliza a rede para dar mais comodidade e facilidade aos clientes, possibilitando que estes resolvam seus problemas sem ter que sair de suas casas. No entanto, oferecer serviços bancários na internet também atrai os criminosos, que se utilizam dela para o cometimento de fraudes.

É patente a enormidade de situações que envolvam a informática e a vida em sociedade, fazendo nascer aí, relações jurídicas, ficando clara a necessidade de legislações específicas para a informática e internet, seja no que tange a esfera privada ou esfera pública do direito, pois na omissão legal, ficará a cargo dos Tribunais a tarefa de resolver os conflitos não abarcados pela lei, como nos esclarece Lóren Formiga de Pinto Ferreira.

Os aplicadores do Direito tentam enquadrar, na medida do possível, esses atos lesivos aos tipos penais previstos no Código Penal e na legislação esparsa, mas muitas, por não se enquadrarem em nenhum dos tipos penais previstos no sistema jurídico-penal do nosso país, ficam impunes, já que não são consideradas como condutas criminosas e sim como fatos atípicos. (FERREIRA, 2009).

5 A REGULAMENTAÇÃO DA INTERNET NO BRASIL E A CRIAÇÃO DA LEI 12.737/2012

As primeiras normas que visavam regular o serviço de internet foram traçadas em 1995, em nota conjunta do Ministério das Comunicações e do Ministério da Ciência e Tecnologia. Ficou estabelecido que os serviços comerciais da rede caberia à esfera privada.

Até a promulgação da Lei nº 12.737 de 30 de novembro de 2012, não havia uma legislação penal especial e autônoma para regulamentar os crimes cometidos na rede. O que ocorria, então, era uma adaptação da atual parte especial do Código Penal. Mas é importante salientar, conforme lembra Fabrizio Rosa, que:

> Não se deve confundir um crime comum praticado pelo uso ou contra o computador de um ‘crime de informática’ propriamente dito. Daí a necessidade de uma legislação específica para esses delitos “ao formular uma nova categorização, o legislador atrai a atenção da indústria, do mundo acadêmico e do governo para o fato em si que, então, se torna objeto de aprofundada reflexão jurídica e técnica. (ROSA, 2002, p.30).

Entretanto, no ordenamento jurídico brasileiro, existem algumas leis que disciplinam o uso da internet, como a Lei nº 7.232, de 29 de outubro de 1984, que estabelece princípios, objetivos, fins, mecanismos de formulação e diretrizes da Política Nacional de Informática. Foi criado também o Conselho Nacional de Informática e Automação - CONIN, com disposições sobre a Secretaria Especial de Informática - SEI, e os Distritos de Exportação de Informática. Igualmente, foram autorizados a criação da Fundação Centro Tecnológico para Informática - CTI, que institui o Plano Nacional de Informática e Automação e o Fundo Especial de Informática e Automação.

Como destaca Fabrizio Rosa sobre os crimes de informática pelo mundo:

> São poucos os países que possuem uma legislação adequada sobre a criminalidade informática. O Conselho Europeu ocorrido em 03 de setembro de 1989 estabeleceu tipos penais nos quais se basearam as legislações de países como Austrália, Alemanha, Portugal, França e Grécia, por exemplo. (ROSA, 2002 p.31).

Atualmente, existem várias discussões sobre o Marco Civil da Internet (oficialmente chamado de Lei nº 12.965, de 23 de abril de 2014). Esta lei veio para regular o uso da Internet no Brasil, por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede, bem como da determinação de diretrizes para a atuação do Estado. O projeto surgiu em 2009 e foi aprovado na Câmara dos Deputados em 25 de março de 2014 e no Senado Federal em 23 de abril de 2014, sendo sancionado logo depois por Dilma Rousseff.

A ideia do projeto, surgida em 2007, foi adotada pelo governo federal em função da resistência social ao projeto de lei de cibercrimes conhecido como Lei Azeredo, muito criticado sob a alcunha de AI-5 Digital. Após ser desenvolvido colaborativamente em um debate aberto por meio de um blog, em 2011 o Marco Civil foi apresentado como um Projeto de Lei do Poder Executivo à Câmara dos Deputados, sob o número PL 2126/2011.6 No Senado, desde 26 de março de 2014 o projeto tramitou sob o número PLC 21 de 20147, até sua aprovação em 23 de abril de 2014.

O texto do projeto trata de temas como neutralidade da rede, privacidade, retenção de dados, a função social que a rede precisará cumprir, especialmente garantir a liberdade de expressão e a transmissão de conhecimento, além de impor obrigações de responsabilidade civil aos usuários e provedores. No presente trabalho, tendo em vista a questão do marco civil da internet, trataremos das questões referentes à responsabilidade penal no que tange a aplicação do artigo 154-a da Lei 12.737/2012 (Lei Carolina Dieckmann).

6 OS CRIMES INFORMÁTICOS

Pois bem, apesar de o tema contar ainda com escasso material, os doutrinadores costumam utilizar várias nomenclaturas para conceituar os crimes informáticos, como por exemplo, “crimes de computador” (BITTENCOURT, 2000), “crimes via internet” (MIRANDA, 2001) ou “crimes digitais” (CORRÊA, 2000, p. 42). Na pesquisa adotou-se a terminologia “crimes informáticos”, nomenclatura que engloba os crimes cometidos na internet ou simplesmente nos dispositivos informáticos, como notebooks, celulares e pendrives, além de ser a nomenclatura utilizada na lei objeto desse estudo.

Marco Aurélio Rodrigues da Costa afirma que grande parte dos doutrinadores define crime de informática como a conduta que atenta contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela transformação, armazenamento ou transmissão de dados, na sua forma, compreendida, pelos elementos do sistema de tratamento, transmissão ou armazenagem dos mesmos, ou ainda, na forma mais rudimentar. (COSTA, 1997).

Carla Rodrigues Araújo de Castro conceitua crime de informática como:

> É 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. (RODRIGUES, 2003, p. 9)

Já para Marco Aurélio Rodrigues da Costa, o conceito de crimes de informática é:

> Todo aquele procedimento que atenta contra os dados, que o faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão. Assim, pressupõe dois elementos: contra os dados e também através do computador, utilizando-se software e hardware para perpetrá-lo. (COSTA, 1997).

Sendo assim, crimes informáticos são aqueles em que o bem jurídico tutelado pelo Estado é violado com o uso de sistemas informáticos como instrumento, seja através de hardware, seja através de software ou quando os próprios sistemas são o próprio objeto da lesão. Adota-se no presente trabalho o conceito de hardware como sistemas informáticos no aspecto físico ou de máquinas propriamente ditas, e software, como instruções lógicas, como por exemplo, os denominados programas de computador.

6.1 A CLASSIFICAÇÃO DOS CRIMES INFORMÁTICOS

Os crimes informáticos podem ser próprios ou impróprios; próprios quando só podem ser cometidos através da informática ou em razão dela, ou seja, impossível o cometimento de tais crimes sem seu uso, como explicam Patrícia Peck Pinheiro e Victor Auilo Haiakal:

> [...] os crimes digitais próprios, aqueles cometidos contra dados, informações ou sistemas de informação, ao revés dos crimes digitais impróprios, quando os sistemas de informação apenas servem como meio para se praticar o delito. (HAIAKAL; PINHEIRO, 2013).

Para se visualizar mais claramente o instituto, é possível citar o exemplo dos crimes de violação de e-mail, pirataria de software, pichação de homepages, danos a equipamentos e programas através da inseminação de vírus, divulgação de material sigiloso, etc. Por se tratar de uma realidade nova, somada a uma escassa legislação, alguns crimes acabavam sendo considerados atípicos, onde na maioria das vezes, seus autores restavam impunes.

Os crimes informáticos impróprios, por sua vez, não dependem de dispositivos informáticos para se caracterizem, tais dispositivos servem como meros instrumentos para o cometimento de crimes que já se encontram tipificados em nossa legislação, a exemplo dos crimes contra a honra, patrimônio etc.

As classificações para os crimes informáticos estão longe de serem uniformes, pois os crimes informáticos podem ser comum, puro ou misto. Crime de informática comum é aquele em que o agente usa o sistema informático apenas como instrumento para o cometimento de um crime comum tipificado na lei, pois pode ser perpetrado por outro meio, como por exemplo, o crime de estelionato.

Crime de informática puro é aquele em que o agente visa especificamente o sistema informático em todas as suas formas, hardwares e softwares, computadores e seus dados, onde o agente pode atentar física ou tecnicamente contra tais sistemas.

Por último, os crimes de informática mistos são aqueles em que o agente visa um bem juridicamente protegido diverso da informática, mas o crime só se consuma por meio do uso de um sistema informático, como por exemplo, uma transferência ilícita de valores bancários com o uso da internet.

6.2 AS ESPÉCIES DE CRIMINOSO NA ERA DIGITAL

Na lição de Sandra Gouvêa os primeiros criminosos digitais surgiram na década de 1970, e eram os programadores, pois estes profissionais tinham alto conhecimento técnico no manuseio de computadores, algo muito dificultoso na época. (GOUVÊA, 1997, p.60).

As primeiras fraudes bancárias datam da década de 80, onde os próprios funcionários apropriavam dos valores das instituições, uma vez que tinham acesso às movimentações das contas.

Atualmente, os criminosos são extremamente diversificados, uma vez que a disseminação dos computadores e da internet possibilita que quaisquer pessoas possam praticar crimes informáticos.

6.2.1 O HACKER (WHITE HAT)

O termo hacker é comumente utilizado para designar criminosos digitais, no entanto, deve-se ter cautela, pois são indivíduos com alto conhecimento técnico sobre computadores, programação e sistemas de segurança, e nem sempre cometem crimes.

Suas motivações são muito variadas, incluindo curiosidade, necessidade profissional, vaidade, espírito competitivo, patriotismo, ativismo ou mesmo crime. Hackers que usam seu conhecimento para fins imorais, ilegais ou prejudiciais são chamados crackers.

6.2.2 O CRACKER

Também denominado “hacker do mal” ou “hacker sem ética”, Henrique Cesar Ulbrich e James Della Valle afirmam que esse indivíduo é, normalmente, especializado em burlar as senhas de softwares comerciais a fim de pirateá-los.

Usa seus conhecimentos, ainda, para invadir computadores e sites com propósitos ilícitos. Muitas vezes é excelente programador e pode criar programas que infectem ou destruam por completo sistemas alheios sem deixar vestígios. Notório conhecedor faz uso de ferramentas que explorem vulnerabilidades nos sistemas que pretendam invadir, tendo noções suficientes para improvisar acaso ocorra algum imprevisto. (ULBRICH, 2004, p.30)

6.2.3 O WANNABE (WANNABEE)

É o usuário comum de internet que almeja ser hacker. O termo pode ser utilizado de forma positiva, quando se refere ao indivíduo que estudou por considerável período e está prestes a ingressar em um nível intermediário, antecessor ao de programador.

Este é o ensinamento de Henrique Cesar Ulbrich e James Della Valle (2004, p.29). Na forma pejorativa, trata-se daquele que deseja entrar no âmbito hacker, contudo, não possui mínima noção do que deve ser feito.

6.2.4 O PHREAKER

O conceito dado por Henrique Cesar Ulbrich e James Della Valle (2004, p. 30) do phreaker refere-se ao *hacker* de sistemas telefônicos, que é exímio conhecedor de eletrônica e telefonia e pode fazer chamadas de qualquer local sem, contudo, pagar por elas.

Phreaker é o nome dado às pessoas ou hackers de Telefonia (Phone + Freak ou Phreak). No Brasil pouco se falou a respeito, mas na verdade há muito tempo os Phreakers agem no Brasil, porém tão pouco divulgado. Hoje com a propagação da Telefonia Celular os Phreakers vieram à tona, seja clonando celulares ou realizando escuta telefônica via frequência. Com a opção das operadoras venderem os aparelhos celulares bloqueados para funcionarem apenas para uma determinada empresa, os Phreaks se uniram e resolveram desbloqueá-los em prol da liberdade.

6.2.5 O CARDER

Essa categoria de criminoso se caracteriza pela especialidade em fraudes com cartões de crédito. Este grupo consegue obter listas de cartões válidos em sites que os utilizam, gerando numeração falsa que é reconhecida pela verificação, roubando e clonando cartões verdadeiros, conforme explicam Henrique Cesar Ulbrich e James Della Valle (2004, p.30).

O Carder é um termo amplamente utilizado por pessoas que atuam em grupo ou sozinhas na internet com o intuito de conseguir dados de cartões de créditos para fraudes *on line*. Os grupos de carders (carding) normalmente se reúnem em salas de bate papo IRC

(*Internet Realy Chat*) em servidores instalados em máquinas vulneráveis. Usualmente um carder analisa determinado shopcart em busca de vulnerabilidades, principalmente para baixar (download) o banco de dados com os dados dos clientes da loja (vítima). Após a extração dos dados da loja (vítima), o carder utiliza os dados para compra em outra loja.

Os produtos são entregues a laranjas, chamados por eles de DROP ou Drops. Com a vinda dos sistemas moset (*Verified by Visa*) a vida dos carders passou a ser mais complicada, dando então espaço para a aplicação de novos golpes, como roubo de senhas de bancos, configurando-se o famoso banking.

6.2.6 O WAR DRIVER

Este grupo é mais recente em relação aos demais e se utiliza das inúmeras vulnerabilidades das redes sem fio, conectando-se a elas. Denominação dada por Henrique Cesar Ulbrich e James Della Valle (2004, p. 30).

7 A NOVA LEI DE CRIMES INFORMÁTICOS: LEI "CAROLINA DIECKMANN"

No dia 3 de dezembro de 2012, foi publicada no Diário Oficial da União, a lei nº 12.737 de 30 novembro de 2012, que tipificou delitos informáticos e alterou o Código Penal. A Lei acrescentou primeiramente os artigos 154-A e 154-B, definindo o crime de invasão de dispositivo informática, também alterou a redação dos artigos 266 e 298 do Código Penal, sendo que o primeiro se refere à interrupção de serviço telemático ou de informação de utilidade pública, e o segundo, equipara o cartão de crédito e de débito a documento particular.

Foi apelidada de "Lei Carolina Dieckmann", e através das alterações supracitadas, alterou o Código Penal para tipificar os crimes cibernéticos propriamente ditos (invasão de dispositivo telemático e ataque de denegação de serviço telemático ou de informação), ou seja, aqueles voltados contra dispositivos ou sistemas de informação.

A lei é fruto de projeto apresentado pelo Deputado Federal Paulo Teixeira (PT-SP), cujo trâmite foi acelerado depois da invasão, subtração e exposição na internet de fotografias íntimas da referida atriz. Cuidando-se de nova lei incriminadora, a norma supracitada dispõe em seu art. 4º *vacatio legis* de 120 (cento e vinte) dias, não podendo retroagir para alcançar

condutas pretéritas. A Lei ganhou enfoque, pois antes mesmo de ser sancionada e publicada, já havia sido nomeada de “Lei Carolina Dieckmann”, devido ao caso de enorme repercussão da atriz que deu nome à Lei.

Em maio de 2012, Carolina Dieckmann teve seu computador pessoal invadido por *crackers*, então cerca de 30 fotos íntimas da atriz foram subtraídas. Segundo notícia publicada em 02 de abril de 2013 no site da Revista Veja, para que as fotos não fossem divulgadas, a atriz foi chantageada a pagar 10 (dez) mil reais aos suspeitos. Como a atriz não cedeu às chantagens, suas fotos foram publicadas na internet e rapidamente se espalharam no ambiente virtual.

A partir da pressão midiática, com o caso da atriz e por 2012 ter sido ano de eleições, o projeto tramitou rapidamente e em caráter de urgência, de acordo com o artigo 155 do Regimento Interno da Câmara dos Deputados, conforme se observa abaixo:

> Artigo 155. Poderá ser incluída automaticamente na Ordem do Dia para discussão e votação imediata, ainda que iniciada a sessão em que for apresentada, proposição que verse sobre matéria de relevante e inadiável interesse nacional, a requerimento da maioria absoluta da composição da Câmara, ou de Líderes que representem esse número, aprovado pela maioria absoluta dos Deputados, sem a restrição contida no § 2º do artigo antecedente. (BRASIL, 1989).

A aprovação se deu 10 dias após o ocorrido pela Câmara dos Deputados. Apresentado ao Senado Federal, o mesmo foi aprovado em 30/10/2012 com pequenas emendas, como a mudança do núcleo do tipo do delito do artigo 154-A, que em sua redação original era “*devassar*” foi alterado para “*invadir*”.

Outra emenda proposta pelo Senado e posteriormente aprovada pela Câmara foi acrescentar ao § 1º do referido artigo a expressão “*dispositivo ou*”, como se observa na redação final da Lei: *“§ 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.”* (grifo nosso). (BRASIL, 2012).

O artigo 154-A também sofreu alteração em seu § 3º, deslocando do § 4º a expressão “*se o fato não constitui crime mais grave*”. O Senado propôs a retirada da expressão “*obter vantagem ilícita*”, pois acreditavam que tal frase iria confrontar com os crimes de furto e estelionato que tem o mesmo especial fim de agir, proporcionando assim uma pena mais branda àquela pessoa que utilize a informática como meio para cometer tais crimes. Porém tal

emenda não foi aprovada pela Câmara dos Deputados permanecendo assim a expressão utilizada da redação original.

A rapidez na tramitação do projeto gerou lacunas e inconsistências, como a necessidade de interpretação dos vários verbos utilizados na Lei, os núcleos do tipo "*invadir*", "*obter*", "*adulterar*", "*destruir*", bem como as elementares que constituem a figura típica, tema que será abordado no tópico seguinte.

6.2 OS ASPECTOS CONTROVERSOS A RESPEITO DA APLICAÇÃO DO ARTIGO 154-A DA LEI 12.737/2012

Ao analisar o referido artigo 154-A da Lei 12.737/2012, é possível atestar vários pontos controvertidos, que geram dúvidas quanto à aplicabilidade da norma, onde as impropriedades técnicas geram o risco de culminar na impossibilidade jurídica de punir certas condutas, haja vista a sua atipicidade. Vejamos, pois, o que dispõe o artigo em análise:

> Artigo 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. (BRASIL, 20012).

A redação se refere a ”*dispositivo informático*”, com isso, sabiamente o legislador optou por não apresentar uma lista exaustiva de dispositivos, haja vista a infinidade de dispositivos existentes como *PCs*, *notebooks*, *netbooks*, *tablets*, *pendrives*, cartões de memória, *HDs* externos, *mp3 players* e tantos outros que ainda virão a existir, capazes de armazenar dados passíveis de violação. Refere-se também a “*mecanismo de segurança*”, não apresentando um rol específico, evitando também que novos tipos de mecanismos não se enquadrassem na referida lei.

No entanto, em certos casos poderão surgir dúvidas acerca do que é ou não um “*dispositivo informático*” ou “*mecanismo de segurança*”. A pergunta é: qual o critério a ser usado para distingui-los? A título de exemplo: Seria um roteador um sistema informático? Seria este passível de invasão? Seria o bloqueio de tela ou teclado dos celulares considerado um mecanismo de segurança? Tais dispositivos seriam passíveis de violação?

Vale ressaltar que devemos ter a ciência de que “*invadir*” e “*ter acesso*”, são situações distintas, uma vez que se pode ter acesso a determinados sistemas informáticos sem, necessariamente, invadi-los, como por exemplo, quando clicamos sobre um nome qualquer na lista de usuários do wi-fi, estamos entrando em contato com o roteador (sistema informático) alheio, sem com isso, estarmos invadindo.

Acerca do verbo nuclear do tipo penal, leciona com clareza Renato Opice Blum:

> Este verbo conceitualmente traz a ideia de entrada à força, ingresso hostil, violação de barreira. Portanto, casos de obtenção indevida de dados através de técnicas de engenharia social e outros meios (divulgação de senha pelo próprio titular do bem a terceiros, por exemplo) em tese não estariam enquadrados na tipificação recém-nascida. Isto porque não haveria qualquer violação, mas apenas o acesso não autorizado. (BLUM, 2014).

Lembrando que quem pratica atos de engenharia social é o indivíduo conhecido como *cracker*.

Para se ter a real extensão da imputação penal, faz-se necessário analisar as descrições acerca do tipo penal. De acordo com Renato Opice Blum (2014), importa analisar

os pressupostos da conduta "*invadir*". Este verbo conceitualmente traz a ideia de entrada à *força, ingresso hostil, violação de barreira*. Portanto, a Lei nº 12.737/2012, embora represente certo avanço ao tipificar crimes cibernéticos propriamente ditos, contém inúmeras deficiências e confrontos com o sistema penal e processual penal vigente, o que deve merecer a atenção dos aplicadores. Os crimes cibernéticos propriamente ditos são a porta de entrada para outras condutas criminosas, facilitando a utilização do computador como instrumento para cometer delitos.

O legislador não contemplou a invasão de sistemas, como os de *clouding computing*, optando por restringir o objeto material àquilo que denominou dispositivo informático, sem, contudo, defini-lo. Atividades de comercialização de *cracking codes* e de engenharia reversa de software também não foram objeto da norma. Além das imperfeições na redação dos tipos, as penas cominadas na nova lei são ínfimas se considerada a potencial gravidade das condutas incriminadas, bastando dizer que um ataque de denegação de serviço pode colocar em risco vidas de uma população inteira.

Quanto ao fato de estar conectado ou não à rede também não resta dúvidas, ou seja, o legislador quis proteger o sistema informático do agente invasor, esteja o agente à distância, esteja ele utilizando fisicamente o dispositivo em questão. Como exemplo, podemos citar dispositivos que não estão conectados, um computador sem acesso a internet ou um *pendrive.*

Um ponto importante a observar é a elementar violação indevida de mecanismo de segurança; a elementar indevida deve-se ao fato de que algumas pessoas têm autorização para invadir sistemas, como no caso de funcionários de empresas de segurança digital, que têm como ofício invadir sistemas para testá-los, não se configurando no caso, ilicitude.

Continuando a análise, fica clara a configuração do crime quando o agente o faz por meio de algum artifício que venha a burlar o referido sistema de segurança, por mais simples e frágil que este seja. Entretanto, é muito comum que computadores e periféricos não tenham sistema de segurança e isso ocorre por diversos motivos, por exemplo, opção do proprietário de não proteger o sistema, esquecimento, desconhecimento técnico, impossibilidades técnicas do dispositivo, como os gravadores e reprodutores de áudio, etc. Ademais, alguns dispositivos dependerão de perícia técnica para que se possa constatar a existência ou não de um dispositivo de segurança.

Situação possível e muito comum no ambiente de trabalho, ao qual o sistema informático ficará desprotegido, ocorre quando um usuário ao entrar com sua senha em seu

dispositivo, se abstém de reativá-la após o uso, possibilitando que qualquer pessoa venha a devassar esse equipamento.

Neste exemplo, o usuário que devassou o dispositivo alheio não invadiu o sistema, nem violou dispositivo de segurança, uma vez que o usuário ao não reativar a senha, deixou o sistema exposto (é como se um álbum de fotos fosse deixado aberto em cima da mesa e não quiséssemos que as fotos ali fossem vistas).

O caput do artigo 154-A poderá ser objeto de muita discussão sobre quem seria o "*titular do dispositivo*" invadido. Poderia o mero possuidor do dispositivo ou usuário eventual figurar como sujeito passivo deste delito? O texto da lei mais uma vez não esclarece. Acredita-se no presente trabalho que o sujeito passivo seja somente o proprietário.

Por outro lado, situação diferente ocorre quando o proprietário fornece algum dado que possibilite o acesso alheio, fornecendo voluntariamente meios para que seu sistema seja invadido, como por exemplo, dando sua senha através de meios artificiosos de utilização por um *cracker*, situação que se enquadraria no induzimento a erro, caracterizando assim o crime de invasão de sistema informático.

Outro ponto relevante é a elementar do artigo em estudo "*com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita*". O novo tipo penal deixa claro o elemento subjetivo do tipo, visando assim, punir a conduta dolosa de obter, adulterar ou destruir dados ou informações, ou seja, dolo específico.

Importante ressaltar que o *wannabe*, aperfeiçoa suas técnicas computacionais penetrando nos sistemas alheios simplesmente para testar suas habilidades, ou seja, sem outra finalidade a não ser de ter a satisfação pessoal de ter conseguido penetrar num sistema vulnerável.

Neste caso, analisando o artigo 154-A da Lei 12.737/2012, é de fácil percepção que o elemento subjetivo deste tipo penal é o dolo, a vontade livre e consciente de obter, adulterar, ou destruir dados, sendo assim, o aspirante a hacker ou *wannabe*, que simplesmente entra no sistema, pratica fato atípico, visto que entrou, mas, sem a intenção de obter, adulterar ou destruir dados.

Quanto à autorização expressa, por exemplo, pode-se citar um banco que contrata uma empresa de segurança digital, determinando a esta que invada seus servidores a fim de testar sua proteção. A autorização tácita se dará, por exemplo, ao se contratar um técnico para recuperar o sistema operacional de uma máquina qualquer e este tenha acesso aos dados e

arquivos armazenados neste micro computador. Assim sendo, poder-se-ia caracterizar a autorização tácita também, quando um indivíduo, por vontade própria, não utiliza um dispositivo de segurança em seu equipamento, evidenciando desta forma que não deseja impedir que outrem tenha acesso aos seus arquivos.

Situação mais relevante ocorre no caso de algumas condutas não preencherem o que dispõe o artigo 154-A, uma vez que em certas condutas há ausência de elementares do tipo penal, senão vejamos:

> Artigo 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 [...]

Ao acessar um sistema informático que não conta com dispositivo de segurança, o agente que o faz sem violar qualquer dispositivo, deixa de preencher a elementar do tipo incriminador mediante violação indevida de mecanismo de segurança. Assim, este indivíduo praticou ato atípico por falta da referida elementar, componente imprescindível da conduta delituosa.

Assevera ainda Renato Opice Blum que:

> Com relação à invasão de dispositivo e formas derivadas, encontramos o primeiro ponto para reflexão: a lei restringiu a tipicidade da conduta aos casos em que há a violação indevida de mecanismos de segurança. Assim, podemos entender que todos os dispositivos informáticos não dotados de ferramenta de proteção estariam excluídos do âmbito desta aplicação legal. Além disso, vale pontuar que, como as expressões "mecanismo de segurança" e "dispositivo informático" (só hardwares? E os softwares?) não foram definidas na lei, pode restar dúvidas sobre o completo enquadramento penal de certos casos. (BLUM, 2014).

Fernando Capez explica que as elementares provêm de elemento, que significa componente básico fundamental, configurando assim todos os dados fundamentais para a ocorrência do fato típico, as quais, na sua falta, a figura típica desaparece. (CAPEZ, 2012, p. 381). E reforça o autor sobre o conceito de elementar:

> [...] é todo componente essencial da figura típica, sem o qual esta desaparece (atipicidade absoluta) ou se transforma (atipicidade relativa). Encontra-se sempre no chamado tipo fundamental ou tipo básico, que é o caput do tipo incriminador. (CAPEZ, 2012, p. 475)

Assim, para a caracterização da figura típica elencada no artigo 154-A, haverá a necessidade de que a conduta do agente preencha todas as elementares**, invadir sistema informático + mediante violação + com o fim de obter, adquirir ou destruir dados ou informações**, na falta de um destes elementos, culminará na atipicidade da conduta.

Nesta linha de raciocínio, leciona Rogério Greco:

> Não é incomum que pessoas evitem colocar senhas de acesso, por exemplo, em seus computadores permitindo, assim, que qualquer pessoa que a eles tenha acesso, possa conhecer seu conteúdo. No entanto, mesmo sem a existência de senha de acesso, a ninguém é dado invadir o computador alheio, a não ser que ocorra a permissão expressa ou tácita de seu proprietário. No entanto, para fins de configuração típica, tendo em vista a exigência contida no tipo penal em análise, somente haverá a infração penal se houver, por parte do agente invasor, uma violação indevida do mecanismo de segurança. (GREGO, 2013, p. 601-602).

Se as condutas fossem típicas na ausência de alguma das elementares, fato típico seria o caso em que um indivíduo se conecta a uma rede *wireless* sem senha, onde o sinal do vizinho entra em sua residência, que a utiliza porque não havia senha, sabendo disso ou não. Frise-se que alguns dispositivos se conectam automaticamente a uma rede aberta ou sem sistemas de segurança.

O mesmo ocorrerá, se o agente acessa o sistema informático, mas não causa dano, nem se apropria de dados ou informações, como no exemplo dado acima, onde o aspirante a hacker, conhecido como *wannabe* só penetra num sistema, unicamente por satisfação pessoal, caso em que será restringido o alcance da regra.

À primeira vista, estas questões não parecem ser muito polêmicas, a não ser com a ocorrência de casos concretos, onde é possível antever fartas discussões nos tribunais, fazendo com que a lei possa surtir efeito diverso do pretendido, seja punindo um inocente, seja deixando impune um criminoso. A título de exemplo, suponhamos que “A” perde seu *smartphone* na rua, “B” o encontra. Para que a situação se resolva poderá ocorrer: “A” liga para o próprio aparelho e o recupera ou “B” liga do aparelho encontrado para algum número da agenda. Dependendo do modo como interpretamos a lei, em tese, “B” pode ter invadido sistema informático e incorrido no crime da Lei nº 12.737/2012.

Estas informações precisam chegar ao conhecimento do maior número de pessoas possível, a fim de que possam se precaver, uma vez que os prejuízos materiais são uma parte menor do problema. Possivelmente os maiores e irreparáveis danos versem sobre os aspectos

íntimos da vida pessoal das pessoas, conquistas profissionais ou outros bens de valor incalculável.

Finalmente, para que haja a proteção dos sistemas informáticos e o proveito da nova lei, se faz necessário que se tome o maior cuidado possível para evitar o acesso não autorizado, com o uso de senhas, códigos de acesso, dados biométricos, assim como manter sempre ativos e atualizados os antivírus, *firewalls*, enfim, tudo que possa dificultar ou obstar o acesso indevido pelos criminosos. Caso haja a suspeita de que alguém possa estar tentando invadir um sistema, deve-se comunicar as autoridades e evitar usá-lo, para que se possa preservar as provas digitais nele contidas a serem periciadas, para se chegar ao invasor.

7 CONSIDERAÇÕES FINAIS

Diante do exposto, pode-se concluir que a tecnologia está evoluindo num ritmo assombroso e junto com ela, a informática, cada vez mais presente e essencial na vida das pessoas. A atividade legislativa não está conseguindo acompanhar estas mudanças tecnológicas e as relações jurídicas delas advindas, somada as vezes, pelas pressões da mídia, culminando em um desequilíbrio social. As leis que estão sendo criadas a partir de fatos do cotidiano necessitarão dos avanços no campo do direito, em contrapartida, se o direito não avançar na mesma linha da era digital, as regras que forem criadas terão uma roupagem pouco efetivas, tornando-se inócuas.

Nesse contexto, não é mais suficiente conhecer apenas o direito e as leis; deve-se conhecer os modelos que conduzem o mundo das relações entre pessoas, empresas, mercados, Estados, etc. A postura profissional de estrategista significa assumir um papel determinante para a adequada condução dos negócios no mundo digital. Cabe ao profissional de direito dar os caminhos e as soluções viáveis, pensadas no contexto competitivo e globalizado de um possível cliente virtual-real, convergente e multicultural.

Em linhas gerais, passa a ser importante saber dominar as novas ferramentas e novas tecnologias à disposição, estudar as interrelações comerciais e pessoais que ocorrem na Internet e nas Novas Mídias Interativas. Além disso, é necessária uma visão ampla do universo jurídico e entender o movimento de autorregulamentação e sua legitimidade, a substituição de leis por softwares que regulam condutas e comportamentos na rede, as mudanças do conceito de soberania dentro de um mundo globalizado e virtual, a necessidade

de incentivos à livre iniciativa virtual (e-commerce), as questões de importação de bens não materiais via Internet e seu impacto macroeconômico, as situações de consumidores virtuais, dentre outros aspectos.

No que diz respeito às infrações ocorridas por meio da internet, a legislação brasileira jurídico-penal ainda é incipiente, não tutelando todos os bens jurídicos ameaçados com a utilização da TI (Tecnologia da Informação). Contudo, esse fato não impede o desenvolvimento do trabalho dos órgãos competentes em articular ações no enfrentamento dessa nova modalidade delitiva. Enquanto houver por parte da legislação penal tal omissão, não serão considerados crimes, como de fato são. Ademais, seus agentes sempre serão agraciados com o benefício da impunidade, pois no direito penal não se pode atribuir uma pena, ou impor uma sanção a uma conduta que o ordenamento penal não considere expressamente como criminosa, mesmo que tal conduta produza prejuízos financeiros ou atente contra a integridade humana, bens resguardados pelo direito penal.

É importante observar que a atividade legislativa deve ocorrer de forma precisa, com estudos cuidadosos e com auxílio conjunto dos especialistas da áreas jurídica e informática, para evitar incoerência e dificuldades na aplicação da lei, evitando fartas discussões nos tribunais, impunidades ou injustiças, além da análise da real necessidade da intervenção do Direito Penal. Saber estabelecer estratégias jurídicas eficientes no mundo cada vez mais digital e virtual é condição de sobrevivência do profissional do direito, uma vez que cada vez mais o tempo e a tecnologia atuam de modo a exigir celeridade e flexibilidade nas soluções jurídicas. A questão que se coloca é de eficácia. Para isso, devemos antever os acontecimentos e criar soluções flexíveis, que sobrevivam ao tempo.

Por fim, registre-se que essas mudanças vieram para ficar, e muitas outras estão por vir, e, cada vez mais, uma visão global com uma atuação de estrategista será exigida dos profissionais do Direito, de modo a trazer soluções para o âmbito de uma sociedade globalizada, convergente, digital e em constante mudança.

REFERÊNCIAS

BLUM, Renato Opice. **Crimes eletrônicos – a nova lei é suficiente?** fev. 2013. Disponível em: < http://www.migalhas.com.br/dePeso/16,MI172711,101048-Crimes+eletronicos+a+nova+lei+e+suficiente> Acesso em: 10 jun. 2014.

BRASIL. Câmara dos Deputados. Resolução nº 17, de 1989. Aprova o Regimento Interno da Câmara dos Deputados. **Diário do Congresso Nacional.** set. 1989.

BRASIL. **Código Penal.** Obra coletiva de autoria da Editora Saraiva com a colaboração de Luiz Roberto Curia, Livia Céspedes e Juliana Nicoletti. 18. ed. São Paulo: Saraiva, 2012.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília: Senado, 1988.

BRASIL. Lei nº 9.099, de 26 de setembro de 1995. Dispõe sobre os Juizados Especiais Cíveis e Criminais e dá outras providências. **Diário Oficial da União**, Brasília, 27 set. 1995.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do artigo 5o, no inciso II do § 3o do artigo 37 e no § 2o do artigo 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências. **Diário Oficial da União**, 18 nov. 2011.

BRASIL. 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. **Diário Oficial da União**, Brasília, 31 dez. 2012.

BRASIL. **Senado Federal.** Quadro Comparativo do Projeto de Lei da Câmara nº 35, de 2012 (nº 2.793, de 2011, na casa de origem). Elaborado pelo Serviço de Redação da Secretaria-Geral da Mesa do Senado Federal. Disponível em: < http://www.senado.gov.br/atividade/materia/getPDF.asp?t=113982&tp=1> Acesso: em 09 ago. 2013.

BRASIL. **Senado Federal.** Parecer nº 1.053, de 2012. Da COMISSÃO DE CIÊNCIA, TECNOLOGIA, INOVAÇÃO, COMUNICAÇÃO E INFORMÁTICA, sobre o Projeto de Lei da Câmara nº 35, de 2012 (na origem, PL nº 2793, de 2011), que dispõe sobre a tipificação criminal de delitos informáticos, altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, e dá outras providências. Disponível em: < http://www.senado.gov.br/atividade/materia/getPDF.asp?t=113638&tp=1> Acesso: em 09 jun. 2013.

CABETTE, Eduardo Luiz Santos. **Primeiras impressões sobre a Lei nº 12.737/12 e o crime de invasão de dispositivo informático.** Jus Navigandi, Teresina, ano 18, n. 3493, 23 jan. 2013 . Disponível em: <http://jus.com.br/artigos/23522>. Acesso em: 13 set. 2013.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. 2. ed. Rio de Janeiro: Lumen Juris, 2003

CIVITA, Victor. **Informática**. São Paulo: Nova Cultural, 1986.

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

COSTA, Marco Aurélio Rodrigues da. **Crimes de Informática.** Jus Navigandi, Teresina, ano 2, n. 12, 5 maio 1997 . Disponível em:<http://jus.com.br/artigos/1826>. Acesso em: 18 nov. 2013.

FERREIRA, Aurélio Buarque de Holanda. **Novo dicionário da língua Portuguesa**. 2ª Ed., Rio de Janeiro: Nova Fronteira, 1986.

GOUVÊA, Sandra. **O Direito na Era Digital: crimes praticados por meio da informática**. Rio de Janeiro: Mauad, 1997.

GRECO, Rogério. **Curso de direito penal**. volume II: parte especial, artigo 121 a 154-B. 10. ed. rev. ampl.. e atual. Niterói: Impetus. 2013.

LAKATOS, Eva Maria. MARCONI, Marina de Andrade. Fundamentos de Metodologia Científica. 4ªed. rev.ampl.. São Paulo: Atlas. 2001.

MIRANDA, Marcelo Baeta. **Abordagem dinâmica aos crimes via Internet**. Jus Navigandi, Teresina, ano 4, n. 37, 1 dez. 1999 . Disponível em:<http://jus.com.br/artigos/1828>. Acesso em: 18 nov. 2013.

MOURA, Pâmela Aline Rocha. **Crime cibernético e seus aspectos no universo jurídico.** Disponível em: <http://www.unipac.br/site/bb/tcc/tcc-388a1273480aa73d54b0c9bb36ffff61.pdf>. Acesso em: 10 jun. 2014.

PECK, Patrícia. **Direito Digital e os novos desafios para o profissional do direito.** Disponível em: <http://www.sedep.com.br/?idcanal=24798>. Acesso em: 10 jun. 2014

PINHEIRO, Patricia Peck. **Direito digital**. 2. ed. rev., atual. e ampl. São Paulo: Saraiva, 2007.

PINHEIRO, Patrícia Peck. HAIAKAL, Victor Auilo. **A nova lei de crimes digitais.** abril. 2013. Disponível em: < http://www.gazetadopovo.com.br/vidapublica/justica-direito/artigos/conteudo.phtml?id=1362035&tit=A-nova-lei-de-crimes-digitais> Acesso: em 10 set. 2013.

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

SÃO PAULO. Ministério Público do Estado de São Paulo. Nota Técnica. **Nova lei de crimes cibernéticos entra em vigor.** Boletim nº 132, abril 2013. Disponível em: <http://www.mp.sp.gov.br/portal/page/portal/cao_criminal/notas_tecnicas/NOVA%20LEI%20DE%20CRIMES%20CIBERN%C3%89TICOS%20ENTRA%20EM%20VIGOR.pdf> Acesso em: 20 set. 2013.

ULBRICH, Henrique Cesar. VALLE, James Della, Digerati, **Universidade Hacker.** 3. ed. São Paulo: 2004.