UNIVERSIDADE FEDERAL DE SERGIPE

CENTRO DE CIÊNCIAS SOCIAIS APLICADAS

DEPARTAMENTO DE DIREITO

JÔLINE CRISTINA DE OLIVEIRA

O CIBERCRIME E AS LEIS 12.735 E 12.737/2012

São Cristóvão – SE

2013

JÔLINE CRISTINA DE OLIVEIRA

O CIBERCRIME E AS LEIS 12.735 E 12.737/2012

Trabalho de Conclusão de Curso apresentado como pré-requisito para a conclusão do curso de Bacharelado em Direito do Departamento de Direito da Universidade Federal de Sergipe.

Orientadora: Profª. Drª. Daniela Carvalho Almeida Costa

São Cristóvão

2013

JÔLINE CRISTINA DE OLIVEIRA

O CIBERCRIME E AS LEIS 12.735 E 12.737/2012

Trabalho de Conclusão de Curso apresentado como pré-requisito para a conclusão do curso de Bacharelado em Direito do Departamento de Direito da Universidade Federal de Sergipe.

Aprovada em _____/_____/_____

Banca examinadora

_____

Profª. Drª. Daniela Carvalho Almeida da Costa

_____

Prof(a). -

_____

Prof(a). -

Dedico esse trabalho

A Deus,

A minha sempre positiva,

mãe, e minha avó.

Que agüentaram as noites

em claro!

RESUMO

O presente trabalho tem como objetivo dispor sobre o cibercrimes e as Leis 12.735 e 12.737/2012, criadas com o intuito de combater essas condutas danosas. Desta maneira, intenta-se explorar o universo cibernético de modo a chegar ao conceito de cibercrime, seu significado e sua origem, suas facetas. Em seguida, será demonstrado como esses atos ilícitos maculam a sociedade moderna, e a quem compete o seu julgamento. Nesse caminho, objetiva-se compreender o processo que levou a elaboração dos projetos legislativos que acabaram transformados nos diplomas normativos acima citados. Como também, as razões que levaram a aprovação das novas normas penais: a pressão midiática, a ocorrência de ataques cibernéticos coordenados, a situação de vulnerabilidade do país. O que influenciou e principalmente aquilo que determinou a criação das Leis. A partir daí, parte-se para uma análise de cada diploma legal, de modo a destrinchar o seu conteúdo, a fim de visualizar suas características, a intenção legislativa e interpretação do texto dos novos tipos penais. Por fim, o presente trabalho irá traçar as perspectivas trazidas com os novos diplomas legais, e as mudanças para aqueles que de alguma forma utilizam os sistemas informáticos.

PALAVRAS-CHAVE: Cibercrime. Leis 12.735 e 12.737/2012 . Tipos Informáticos.

ABSTRACT

The present paper aims to provide for the cybercrimes and Laws 12.735 and 12.737/2012, created in order to combat these harmful behaviors. Thus, attempts to explore the cyber universe to arrive at the concept of cybercrime, its meaning and origin, its facets. Then it will be demonstrated how these unlawful acts tarnish the modern society, and who should his trial. In this way, we aim to understand the process that led to the drafting of legislative bills that eventually transformed into normative texts cited above. As well, the reasons that led to the adoption of new criminal laws: the media pressure, the occurrence of coordinated cyber attacks, the vulnerability situation of the country. What influenced and mostly what led to the creation of Laws. From there, we proceed to an analysis of each statute in order to unravel its contents in order to view its features, the legislative intent to interpret the text of new crimes. Finally, this paper will outline the perspectives brought to the new laws, and changes to those that somehow utilize computer systems.

KEY-WORDS: Cybercrimes. Laws 12.735 e 12.737/2012. Computer types.

SUMÁRIO

1. INTRODUÇÃO

Recentemente foram aprovadas pelo Congresso Nacional e sancionadas pela Presidenta Dilma Rousseff, duas leis criadas com o intuito de combater os chamados cibercrimes.

A elaboração dos novos diplomas penais foi, em grande parte, influenciada pela mídia, após um caso de grande repercussão envolvendo uma atriz famosa. Esta veio a sofrer uma ação ilícita perpassada no universo cibernético, mas que operou reflexos no mundo material.

Ocorre que o fato em questão não pode ser punido, pois não havia previsão para tais ações até então. Esse fato em conjunto com outros, também noticiados, levou ao debate os chamados cibercrimes ou crimes cibernéticos, em sua patente necessidade de tipificação.

A sociedade brasileira, inserida no conjunto da modernidade, é dependente dos meios cibernéticos para o seu bom funcionamento. Ocorre que o franco desenvolvimento tecnológico que o país tem vivenciado não é acompanhado pela atualização de suas leis. Dentre estas, está o Código Penal, aprovado na década de 1940, quando o meio de comunicação mais expressivo era o rádio.

Nos últimos anos o país tem relutado à idéia de elaborar figuras penais que tipificassem as ações praticadas através dos dispositivos cibernéticos. Tendo por muito tempo se apoiado no entendimento de que todas as más condutas existentes no meio virtual poderiam ser reprimidas apenas com a legislação penal em vigor.

No entanto, observou-se que a disponibilização de dados e informações pessoais nesse universo, fazia nascer uma, ou melhor, até várias existências virtuais, e esse mundo paralelo possuía os próprios valores.

Deste modo, foram surgindo condutas ilícitas que só poderiam ser praticadas dentro desse ambiente, e que desta forma só surtiam seus resultados nele, mas traziam efeitos ao mundo material. Assim, o universo cibernético, na vertente dos cibercrimes, passou a fazer parte da vida cotidiana.

Por todo o exposto é preciso entendê-los, saber o que significam, quais as suas características e como evitá-los. E desta maneira, ter em conta o que eles causam para o país e o que tem sido feito para combatê-los.

Nesse contexto, o primeiro o segundo capítulo trará as nuances do mundo cibernético, demonstrará como ele funciona, quais as suas influências, fará uma breve comparação com o universo material, para em seguida visualizar como ele veio a se tornar tão necessário a vida humana e como as sociedades passaram a resguardar os seus bens da vida, e confiar sua segurança aos sistemas telemáticos.

Ainda no segundo capítulo será traçado um perfil das condutas ilícitas e delitos cibernéticos mais praticados. No mais, será observada a jurisdição e competência para julgamento e a atribuição para investigação desses delitos.

O terceiro capítulo retratará o processo de aprovação das normas penais. Para isso, ele demonstrará as etapas pelas quais passaram os projetos de lei, o que permaneceu e o que foi deixado para trás. Também serão apontados os fatos que levaram a criação e aprovação das leis, de maneira a destacar o que impulsionou as sanções dos diplomas.

Por sua vez, o quarto capítulo fará uma análise detalhada das novas normas penais, de modo a destacar o que elas representam dentro do contexto em que serão inseridas, como se dará a sua interpretação e o que será alterado coma sua vigência.

Já o capítulo cinco traçará as perspectivas diante da aprovação dos novos diplomas penais. Nessa esteira, será apontado o que se espera que as novas leis venham refletir, qual a vontade social e legislativa em sua existência. Nesse ínterim, também será destacado o que mudará com a vigência das novas normas, assim, indicar quais os novos procedimentos a ser seguidos nas investigações e até na utilização das novas tecnologias.

Nesse diapasão, faz-se necessário analisar os novos diplomas penais, em todas as suas vírgulas, de modo a interpretar a que se destinam. Como também, supor como eles influirão no comportamento social quando passarem a ser aplicados no caso concreto.

Enfim, o Estado brasileiro entrou na era dos delitos tecnológicos, e o presente trabalho vai mostrar como ele o fez.

2. DO CIBERCRIME

Neste capítulo traçaremos a idéia de cibercrime. O que motivou a existência desse termo e o que retrata esse neologismo criado através dos verbetes cibernética e crime. Palavras de tamanha distinção, tanto pelo que representam quanto pelo tempo que a humanidade as conhece.

Compreenderemos, então, como esse conceito veio a ser criado e como ele passou a representar um claro sentido às condutas ilícitas praticadas no meio cibernético. Com o intuito de facilitar o entendimento, de início traremos à tona o chamado mundo cibernético.

2.1 DO MUNDO CIBERNÉTICO

A humanidade tem passado por uma incrível revolução tecnológica nas últimas décadas. Há uma crescente interdependência entre o ser humano e a máquina, onde um envia comandos e o outro executa em uma bem sucedida transferência de tarefas do primeiro para o segundo.

Essa interação ou interdependência resume bem o mundo cibernético. O ser humano delega à máquina o processamento de informações ou comandos através da lógica, assim, uma inteligência não biológica ou artificial substitui o raciocínio de vários homens na execução de inúmeros trabalhos.

2.1.1 CONCEITO

Segundo o dicionário Aurélio (FERREIRA, 2004) a cibernética consiste na "Ciência que estuda as comunicações e o sistema de controle não só nos organismos vivos, mas também nas máquinas", sua origem deriva do grego *kybernetiké*, *i. e.*, *téchne kybernetiké* ou "a arte do piloto".

Cibernético, portanto, é tudo que tem relação com essa ciência, muitas vezes reconhecidos por fazer a alusão ao trazerem o elemento *ciber,* do inglês *cyber,* como prefixo, tal qual o termos *ciberespaço*, ou mundo virtual, a *cibercultura*, e os *ciborgues*, elementos muito bem representados pela ficção científica em filmes como *"Matrix" (*MATRIX, 1999) e nos livros de Isaac Asimov, *"Eu, robot"* e *"O homem bicentenário"* (ASIMOV, 2004 e 1997), obras também adaptadas para o cinema.

O advento da internet, rede de computadores interligados como uma teia, trocando informações simultaneamente, transformou a interação homem e máquina de um modo até então imaginado apenas como roteiro de ficção. A comunicação instantânea encurtou as distâncias e acelerou a globalização, o computador passou a ser ferramenta indispensável para a elaboração das mais diversas atividades e adentrou as casas. Além disso, estar *on-line*, expressão que significa estar conectado com a internet, tornou-se algo necessário na sociedade contemporânea.

Pensar que toda essa interação começou com uma máquina de calcular rudimentar. Segundo Maciel Colli "o primeiro modelo de computador data de 1839 e é associado à máquina de calcular de Charles Barbbage, na qual o uso de cartões perfurados permitia a realização de cálculos matemáticos". (2010, p. 31 *Apud* WINEGRAND *et al* 1996)

O aumento geométrico da capacidade de armazenamento e processamento de informações impulsionou o uso da tecnologia em todos os campos da vida humana. A vida biológica passou a ser acompanhada pela virtual, esta representada pelo perfil das pessoas, criado através de informações fornecidas por elas aos sistemas. Assim, passamos a viver duas realidades, a existência física e a imaterial, presente em meio ao ciberespaço, esse ambiente de intensa troca de dados.

A imagem das máquinas como aliadas do ser humano evoluiu a ponto de delegarmos a elas as tarefas mais relevantes. Pautados na confiança gerada pela

possibilidade mínima de erros, os sistemas operacionais auxiliam na condução e coordenação dos mais variados processos.

E quando se fala em saúde, a contribuição da cibernética em meio à biônica tem melhorado e até prolongado a vida. Como se vê da utilização de mecanismos de respiração artificial e do uso de próteses, essa última a própria interação homem/máquina que avança os limites do meio orgânico para o inorgânico, e cria os ciborgues no entender de muitos.

O cibermundo ou mundo cibernético constitui-se nesse ambiente de intensa troca de informações entre indivíduos vivos e mecanismos não biológicos, independente de sua localização geográfica, onde o homem alia-se à máquina como o comandante de um navio a navegar pela rede de dados que cria a existência virtual.

2.1.2 DA CORRELAÇÃO COM OS BENS DA VIDA

Como já foi dito nas páginas anteriores, a crescente confiabilidade nos mecanismos não biológicos conduziu a sociedade contemporânea a delegar-lhes tarefas das mais relevantes. Assim, eles passaram a resguardar os bens da vida a que o homem dá valor, e dentre eles aqueles que o direito considera essenciais.

Estamos falando aqui de valores biológicos e sociais, os quais regem o viver contemporâneo. Dentre eles, a saúde, a intimidade, a segurança, liberdade, propriedade e tantos outros.

Passamos para o meio tecnológico ou virtual todos os dados que entendemos ser importantes, desobrigando-nos de guardá-los em meios físicos e/ou na memória. Desta forma, bancos de dados nos mantém atualizados sobre nós mesmos.

É inegável a dependência da sociedade moderna desses meios informáticos. Basta pensar nos bancos e no sistema financeiro como um todo. Neles todo o seu funcionamento está baseado no processamento de dados por centrais computacionais, desta maneira é possível utilizar todos os mecanismos disponíveis por meio eletrônico.

Assim como salvaguardamos o nosso sistema financeiro, usamos essa inovação para manter segura nossa saúde, com o uso de mecanismos como corações artificiais e monitores de glicose, nosso sistema jurídico, com a implantação de processos virtuais, e tudo o mais que entendemos ser importante a ponto de merecer a confiabilidade e a rapidez dos eletrônicos.

Um exemplo notório de como a tecnologia foi utilizada para resguardar valores no país, pode ser lembrado de dois em dois anos com as eleições. A urna eletrônica e, por conseqüência, o voto eletrônico, causaram uma enorme revolução no modo de assegurar a liberdade e a democracia.

Ademais, o próprio conhecimento tecnológico consiste em algo de grande importância, por conta disso costuma-se protegê-lo por senhas e demais mecanismos de segurança eletrônica.

Assim, chegamos mais perto do conceito de cibercrime, uma vez que delineamos o significado de cibernética e o seu campo de ação em meio aos bens da vida.

2.2 DOS CRIMES E CONDUTAS ILÍCITAS PRATICADAS NO MEIO CIBERNÉTICO

São incontáveis as condutas ilícitas que podem ser praticadas no meio cibernético ou através dele. Praticamente todos os comportamentos realizados no mundo físico podem ser levados a efeito pelo mundo virtual.

No entanto, há alguns procedimentos ilícitos que só podem ser realizados através dos meios eletrônicos, por sua especificidade, ou como na maioria dos casos, porque o bem juridicamente relevante é fruto dessa revolução tecnológica e só existe nesse espaço imaterial.

2.2.1 CIBERCRIMES E OUTRAS CONDUTAS ILíCITAS

Chegamos, então, ao conceito de cibercrime, trata-se, pois, de conduta que vem ferir um bem da vida juridicamente tutelado, ou seja, uma conduta ilícita já tipificada para as ações no mundo físico, contudo, agora praticada através do processamento de informações, como meio determinante para a sua consecução.

Ou quando o meio eletrônico não é apenas um canal indispensável para a prática, mas também onde a ação delituosa gera seus efeitos, não sendo mais necessária uma consequência fora do mundo imaterial.

Segundo Paulo Lima, esse conceito pode ser entendido como:

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

Embora se tente enquadrar todas as ilicitudes presentes no meio cibernético nas figuras penais típicas, dado a constante evolução tecnológica, e com ela a transformação da sociedade, isso não é possível, pois o direito penal tende a ficar obsoleto.

O diploma penal pátrio, em vigor desde 1940, não consegue abarcar todos os novos valores da sociedade contemporânea, habituada com o uso de computadores e outros mecanismos. Daí a necessidade de tipificar e assim proteger, através da tutela penal, esses novos bens da vida, tal qual o direito a informação, consubstanciado nos dados disponibilizados em páginas de internet, sem deixar de lado os princípios que norteiam a criminalização das condutas, dentre eles o da intervenção mínima.

Como observado, a punição dessas condutas depende ainda muito da interpretação das normas penais já existentes. A hermenêutica jurídica reveste-se de fator determinante para caracterizar as figuras criminosas. Conforme Zaniolo: “A interpretação é elemento fundamental para os “crimes” modernos, ainda quando a

grande maioria desses ainda não possui tipificação legal e deve ser enquadrada no ordenamento jurídico existente, caso aplicável.” (2007, p. 37)

Há uma gama de comportamentos ilícitos conhecidos que causam enormes transtornos no meio eletrônico e, por conseguinte, na vida daqueles que baseiam suas atividades neles. As mais comuns são o furto de dados, a falsificação de documentos e a invasão de sistemas.

Dentre esses, citam-se o chamado “furto” de sinal de TV por assinatura, algumas vezes considerado como estelionato, pois o sinal nesse caso não pode ser equiparado à energia para a aplicação do §3º, Art. 155, que tipifica o crime de furto. Outro exemplo parecido e também muito comum de ser encontrado é o “furto” de sinal de internet, nesse caso a rede de transferência de dados é desviada de maneira clandestina, entre outros.

A clonagem de dispositivos através da cópia de dados pessoais consiste em uma grave questão dos tempos atuais. A proteção dessas informações vem a ser uma grande ambição contemporânea, tendo em vista o repasse constante do conteúdo pessoal e, portanto, sigiloso, aos mais variados sistemas.

A clonagem de cartões de crédito, ou seja, a criação de um cartão magnético utilizado para o pagamento de mercadorias e serviços a partir de dados retirados de outro, exemplifica o perigo nefasto da falta de segurança para com as informações.

Esse tipo de delito era responsável por uma imensa perda de valores monetários para as instituições financeiras, e era fortalecidos pela ausência de punição aos que utilizam mecanismos capazes de propiciar a captura desses dados.

Isso ocorria, pois até então não havia a possibilidade de enquadrar essas ações como fraude ou outro tipo penal já conhecido, tendo em vista que se corria o risco de enveredar pelo caminho da analogia *in mallam partem*, o que não é aceito pelo direito penal, por força do princípio da legalidade.

A forma de coibir tais ações ocorria após o uso do objeto clonado, quando ficava presente à figura do estelionato ou furto, a depender da interpretação judicial, visto que o crédito que vem a ser utilizado estava disponível apenas pra o real fornecedor dos dados.

Para conseguir essas informações sigilosas, indivíduos conhecidos como *hackers* utilizam-se de seus conhecimentos telemáticos para encontrar fragilidades nos sistemas, *softwares* como conhecidos, e assim ter acesso a dados sigilosos. Já outros, os chamados *crackers,* usam esses mesmos saberes para “quebrar” as

barreiras de segurança sistêmicas. O uso do termo *hacker* seja comum para designar os dois tipos de malfeitores, como se lê no excerto:

> De qualquer modo, ainda que não se tenha chegado a um consenso quanto ao conceito doutrinário de delito informático, os criminosos eletrônicos, ou ciberdelinqüentes, já foram batizados pela comunidade cibernética de *hackers, crackers* e *phreakers*.
> (...)
> Embora no *underground* cibernético, essas diferentes designações ainda façam algum sentido e tenham importância, o certo é que, hoje, para a grande maioria das pessoas, a palavra *hacker* serve para designar o criminoso eletrônico, o ciberdelinqüente. E isto mesmo na Europa e nos Estados Unidos, onde já se vem abandonando a classificação um tanto quanto maniqueísta acima assinalada. (ARAS, 2001)

São inúmeros os métodos usados por esses indivíduos para de alguma maneira “enganar” os *softwares* e aqueles que os utilizam. Entre eles estão o envio de “vírus”, programas lesivos ao sistema, capazes de corrompê-los causando-lhes problemas estruturais e de se replicarem sozinhos, daí a analogia com os “vírus” biológicos.

Outros meios foram desenvolvidos através de princípios similares, como: o “cavalo de tróia”, *worm, keylogger, phishing scam* e a famosa engenharia social. Essa se constitui no uso de informações pessoais de um indivíduo para com isso descobrir suas senhas de acesso aos sistemas.

Isso ocorria continuamente, muito porque a invasão de um banco de dados e a cópia dessas informações não configurava nenhum delito até então, o que vai mudar com os novos diplomas penais, mas isso será melhor discutido a frente, quando da analise dos novos tipos penais criados com a lei que disciplina os crimes cibernéticos.

2.2.2 JURISDIÇÃO E COMPETÊNCIA

O poder-dever do Estado de coibir os cibercrimes, ou seja, a jurisdição existente sobre eles para reprimi-los, e a competência de processamento dos casos,

leva em consideração as regras presentes no Art. 69 e seguintes do Código de Processo Penal, com algumas especificidades.

Muito embora as condutas perpassadas no meio informático possam surtir efeitos em todo o mundo, pois podem ser acompanhadas de praticamente todos os pontos dele na rede *web* (teia de troca de informações na internet) entende-se que o local onde elas possuam maior repercussão, é na sua origem. Segue-se, pois, a regra do local da consumação do crime ou do resultado da ação.

Malgrado tenha-se tentado deslocar a competência desses delitos para a Justiça Federal, com argumento da constante transnacionalidade dos crimes, restou impossibilitada a medida, ante a ausência dos requisitos presentes no Art. 109, incisos IV e V da Constituição Federal.

Em seu livro sobre crimes modernos, Paulo Zaniolo discorda a respeito desse entendimento, vejamos:

> A nosso ver, mesmo não se enquadrando nas hipóteses legais dos incs. IV e V do art. 109 da CF/88, evidente o requisito da transnacionalidade desses delitos, exigido pelo mencionado inc. V, de vez que a conduta do agente poderá implicar no acesso de informações por quaisquer outros usuários da grande rede, em locais diferentes (em qualquer local do mundo), o que Guilherme de Souza Nucci denomina *consumação dúplice* [...] (ZANIOLO, 2007, 45)

Alguns delitos, no entanto, por sua natureza acabam atraídos para a Justiça Federal. Nessa categoria estão presentes os já citados delitos transnacionais e aqueles que preenchem os requisitos presentes nos incisos IV e V do art. 109 da Constituição Federal.

Também atraem a competência federal, os ilícitos que o país se comprometeu a combater por tratado ou convenção internacional, como o racismo e aqueles relacionados com a exploração infantil, tal qual o crime a divulgação de pornografia infanto-juvenil.

Assim, os delitos são investigados e julgados em sua maioria pelos órgãos estaduais, o que traz a necessidade de especialização para melhor entendê-los.

3. DA APROVAÇÃO DAS LEIS 12.735 E 12.737/2012

Os Projetos de Lei voltados á coibição de ilícitos praticados através do meio virtual, cibernético, ganharam relevo e importância juntamente com a expansão das novas tecnologias no país.

Malgrado tenham sido desacreditados em razão do entendimento dominante de que tal iniciativa representava um inchaço inútil à legislação penal, tendo em vista que se creditava que as ações ilícitas do meio cibernético poderiam ser combatidas apenas com a legislação penal já existente, percebeu-se que era necessária a modernização dos tipos penais para a que os cibercrimes não fugissem ao controle.

Com o tempo e, sobretudo, com o aumento da dependência da sociedade brasileira para com os meios telemáticos, percebeu-se que esse novo universo não deveria apenas ser tratado como uma versão virtual do mundo palpável, mas uma dimensão que permite a coexistência de algo com sigo mesmo.

3.1 O HISTÓRICO EM VOLTA DOS PROJETOS DE LEI

3.1.1 O PL 84/1999 (PL 89/2003) E A APROVAÇÂO DA LEI 12.735

O processo legislativo que levou à aprovação do diploma legal 12.735, de 30 de novembro de 2012, percorreu um longo caminho de enormes modificações até chegar ao modelo sancionado.

O PL 84/1999, também conhecido como Projeto Azeredo, pois foi o então senador Eduardo Azeredo, o responsável por elaborar o projeto substitutivo do Senado Federal (89/2003), pairou por vários anos como uma tentativa de censura ao avanço tecnológico no país, motivo pelo qual chegou a ser chamado de AI-5 Digital.

Esse mal aclamado rascunho legislativo passou por sucessivas transformações realizadas pelos ocupantes das duas casas do Congresso Nacional. Inicialmente foi proposto pelo então Deputado Federal Luiz Piauhylino de Melo Monteiro, perante a Câmara dos Deputados. Tratava-se de uma releitura do PL 1713 de 1996, de autoria do então Dep. Cássio Cunha Lima e um grupo de juristas, arquivado em decorrência do fim da sua legislatura.

Os 18 (dezoito) artigos previstos, criavam novos tipos penais compreendidos do Art. 8º ao Art. 14. Nesse sentido, a Seção I, iniciada no Art. 8º trazia as primeiras condutas a serem combatidas no âmbito criminal, descritas como o dano a dado ou programa de computador.

Em seguida, a Seção II, Art. 9º punia o acesso indevido ou não autorizado a computador ou rede de computadores. Já o Art. 10 punia a alteração de senha ou mecanismo de acesso a programa de computador ou dados. A Seção IV, Art. 11, criminalizava a obtenção indevida ou não autorizada de dados ou instrução de computador.

O Art. 12, Seção V do Projeto de Lei, tipificava a violação de segredo armazenado em computador, meio magnético, óptico ou similar. E o Art. 13, Seção VI, penalizava a criação, desenvolvimento ou inserção em computador de dados ou programas de computador nocivos.

Por fim, o Art. 14, Seção VII, trazia a veiculação de pornografia através da rede de computadores, onde na verdade o que se punia era a ausência de aviso sobre o conteúdo e a inadequação dele para crianças e adolescentes.[1]

Como pode ser extraído da simples leitura das condutas descritas como ilícitas, o projeto de lei pecava pela subjetividade das normas abertas ou especificações atécnicas utilizadas para caracterizar as ações. Era patente a ausência de critérios capazes de distinguir o uso adequado da tecnologia das agressões aos bens da vida através e no universo informático.

Tratava-se em verdade, de uma tentativa tênue e crua de resguardar novos valores, os quais a sociedade brasileira passava a eleger na medida que ia aumentando sua dependência em relação a eles.

O arcabouço passou por várias análises das Comissões de Constituição e Justiça (CCJC), de Cidadania Ciência de Tecnologia, Comunicação e Informática

[1] BRASIL. **Projeto de Lei nº 84, de 1999**. Disponível em: <http://www.camara.gov.br/proposicoes.Web/fichadetramitacao?id.Proposicao=15028>. Acesso em: 05 de mar 2013.

(CCTCI) e da Comissão de Segurança Pública e Combate ao Crime Organizado (CSPCCO), quando então foram apensados outros Projetos de Lei – PL nº 2557/2000[2], 2558/2000[3] e 3796/2000[4] – também tendo sido modificado pelo Substitutivo de Relatoria do Deputado Nelson Pelegrino, tendo deixado o formato de lei esparsa para transforma-se em proposta de modificação do Código Penal.

Logo em seguida, o projeto foi enviado ao senado, passando ao ser chamado de PL 89/2003, nomenclatura mais conhecida. Os delitos foram definidos como de ação como penal pública condicionada à representação do ofendido, exceto nos casos em que fossem praticados contra a Administração Direta e Indireta, empresas públicas, sociedades e instituições coligadas, quando então ela passava a ser incondicionada. Como veremos adiante este foi um dos poucos artigos aprovados no processo legislativo, o que poderá ser visto em breve.

Para uns ele representava avanços no combate a essa nova vertente criminal, para outros se tratava apenas de uma tentativa estatal de controlar o desenvolvimento tecnológico, impondo a este, limites não compatíveis com o meio interativo que é o ambiente virtual.

Além disso, seus artigos não punitivos poderiam representar uma ameaça em potencial à liberdade de expressão, ao regular a utilização das informações presentes em redes de computadores através de normas que a depender de sua interpretação, poderiam significar uma forma de censura, e desta maneira, dar margem a um controle estatal sobre a liberdade de expressão.

O projeto previa ainda o aumento em 1/6 (um sexto) a 1/2 (metade) da pena para os crimes ali descritos que fossem praticados no exercício da atividade profissional ou funcional. Somado a isso, estabelecia a criação de setores policiais especializados na investigação dos delitos cibernéticos, o que também será melhor analisado em seguida.

Por fim, o Art. 21 do arcabouço trazia a tão debatida atribuição da Polícia Federal para a investigação das condutas penais descritas no projeto. Já o art. 22

---

[2] BRASIL. **PL 2557/2000**. Disponível em: <http://www.camara.gov.br/proposicaoWeb/fichadetramitacao?idProposicao=18306>. Acesso em: 06 mar 2013.
[3] BRASIL. **PL 2558/2000**. Disponível em: <http://www.camara.gov.br/proposicaoWeb/fichadetramitacao?idProposicao=18308>. Acesso em: 06 mar 2013.
[4] BRASIL. **PL 3796/2000**. Disponível em: <http://www.camara.gov.br/proposicaoWeb/fichadetramitacao?idProposicao=20236>. Acesso em: 06 mar 2013.

listava um série de obrigações que deveriam nortear a atividade dos provedores de internet[5].

Sobre o assunto, em seu livro Maciel Colli afirma: “O curioso é que aqui a falta de precisão técnica fez com que a norma explicativa se restringisse aos provedores, não alcançando os servidores[6] de internet.” (2010, 159)

Ao já reformulado Projeto de Lei foram reunidas as propostas de Projetos Substitutivos do Senado Federal nº 137/2000[7], 76/2000[8] e 89/2000[9], este último contendo o Parecer do então Senador Eduardo Azeredo.

Na época, ele era Relator da Comissão de Ciência e Tecnologia, Inovação, Comunicação e Informática, o Parecer trazia em seu bojo, justificativas para a criação das novas figuras punitivas, entre elas estava o segundo lugar do país na lista daqueles com maior número de incidentes desse tipo, reportados no ano de 2006.

O malfadado Projeto Substitutivo chegou a ser chamado de AI-5 Digital, em referência ao Ato Institucional nº 05 de 1968, implantado pelo Regime Militar, e que tinha a censura das comunicações como sua maior marca.

A sociedade civil organizada acusava a iniciativa legislativa de criminalizar práticas cotidianas na internet, de tornar as redes P2P[10] suspeitas (tipo de rede muito utilizada no compartilhamento de músicas e vídeos), de responsabilizar provedores de acesso a internet pela investigação das ações ligadas a ela, entre outras críticas.[11]

---

[5] Empresas fornecem acesso à internet como serviços agregados de e-mail, hospedagem de blogs etc. **Fornecedor de acesso à Internet**. Disponível em: <http://pt.wikipedia.org/wiki/Fornecedor_de_acesso_%C3%A0_Internet. Acesso: 06 mar 2013.

[6] Computador que controla o acesso de uma determinada rede à internet **O que é um servidor de internet?** Palpite Digital.Com. Disponível em: <http://www.palpitedigital.com/o-que-e-um-servidor-de-internet/>. Acesso em: 06 mar 2013.

[7] BRASIL. **PLS 137/2000**. Disponível em: <http://www.senado.gov.br/atividade/materia/Consulta.asp?Tipo_Cons=6&orderby=0&Flag=1&RAD_TIP=OUTROS&str_tipo=PLS&txt_num=137&txt_ano=2000.> Acesso em: 08 mar 2013.

[8] BRASIL. **PLS 76/2000**. Disponível em: <http://www.senado.gov.br/atividade/materia/Consulta.asp?Tipo_Cons=6&orderby=0&Flag=1&RAD_TIP=OUTROS&str_tipo=PLS&txt_num=76&txt_ano=2000.> Acesso em: 08 mar 2013.

[9] BRASIL. **PLS 89/2003**. Disponível em: <http://www.senado.gov.br/atividade/materia/Consulta.asp?Tipo_Cons=6&orderby=0&Flag=1&RAD_TIP=OUTROS&str_tipo=PLC&txt_num=89&txt_ano=2003.> Acesso em: 08 mar 2013.

[10] Tipo de rede muito utilizada no compartilhamento de músicas e vídeos. **Peer-to-Peer**. Disponível em: <http://pt.wikipedia.org/wiki/Peer-to-peer>. Acesso em: 07 mar 2013.

[11] **Projeto Azeredo: Ato Contra o AI-5 Digital dia 14, em São Paulo, 3 junho de 2009**. Software Livre Brasil. Disponível em: <http://softwarelivre.org/portal/legislativo/projeto-azeredo-ato-contra-o-ai-5-digital-dia-14-em-sao-paulo.> Acesso em: 06 mar 2013.

Esse projeto foi, para desgosto de muitos, mantido em grande parte no Substitutivo do Senado Federal, tendo em vista os motivos já mencionados. Mais uma vez Colli faz uma crítica ao projeto: *"*O PL 89, 2003, do Senado Federal, proposto pelo Senador Eduardo Azeredo, é diploma com teor punitista, repressor e criminalizador muito mais acentuado que o PL 84, 1999, da Câmara dos Deputados. A começar pelo número de tipos penais criados, vinte e um, o triplo do número que o PL originário propunha*"*. (2010, 156-157)

Propunha-se criar as seguintes figuras criminais: a) Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado; b) Obtenção, transferência ou fornecimento não autorizado de dado ou informação; c) Divulgação ou utilização indevida de informações e dados; d) Dano, destruição de dado eletrônico; e) Inserção ou difusão de código malicioso; f) Inserção ou difusão de código malicioso seguido de dano; g) Estelionato eletrônico, quando a difusão facilitasse ou permitisse acesso indevido à rede de computares; h) Atentado contra a segurança de serviço de utilidade pública (informação ou telecomunicação; i) Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema informático; j) Falsificação de meio eletrônico ou documento público; k) Falsificação de dado eletrônico e documento particular.

Também previa a inserção no Código Penal Militar dos delitos citados nos itens a, b, c, g, e, f, além do crime de destruição de dado simples (destruição de dado eletrônico) e dano material ou aparelho de guerra ou eletrônico. O Art. 14 propunha ainda a tipificação da conduta de falsificação de documento ou dado eletrônico quando atentasse a administração ou o serviço militar. Na mesma esteira, o Art. 15 incluía no já descrito crime de favor ao inimigo, a ação de entregar dado eletrônico, ou a perda, destruição, inutilização deste.

O esboço trazia em seu Art. 16, os conceitos de informáticos utilizados para amparar as figuras penais. O Art. 18 de outro modo previa a criação de setores especializados da polícia judiciária. Já o Art. 20 alterava o "caput" do Art. 241 do Estatuto da Criança e do Adolescente, a fim de coibir a prática, por meio da rede mundial de computadores, das condutas já descritas.

Levando-se em conta todo o contexto que se seguiu a apresentação do Projeto Substitutivo, é possível entender que as pressões pela não aprovação do PL 89/2003 acabaram por provocar a rejeição de grande parte dos artigos, de maneira

que foram levados a votação apenas 05 (cinco), relativos ao 1º, 9º (rejeitado e substituído pelo Art. 7º em seu original do Projeto 84/1999), 15, 18 e 19, do substitutivo, aprovados na redação final como Arts. 1º, 2º, 3º, 4º e 5º, respectivamente. A matéria foi encaminhada à sanção da Presidenta da República em 08 de novembro de 2012.

O diploma legal foi então aprovado com veto parcial pela Chefe do Poder Executivo Federal. A justificativa para a não aceitação ao Art. 2º, o qual previa o delito de falsificação de cartão de crédito, foi a não possibilidade de coexistência de dois tipos penais idênticos, tendo em vista a previsão legal na Lei 12.737/2012, aprovada em conjunto, como será observado em breve.

O veto ao Art. 3º, que criava dois incisos no Art. 356 do Código Penal Militar, o qual tipifica o delito de favor ao inimigo, foi justificado pela amplitude do conceito de dado eletrônico, presente na conduta que seria criminalizada, o que poderia inviabilizar a sua aplicação.

Por fim, o Projeto de Lei 84/1999 ou 89/2003, como era mais conhecido, foi transformado na Lei 12.735/2012, contendo 04 (quatro) artigos, tendo sido sancionada em 30 de novembro de 2012 e publicada em 03 de dezembro.

3.1.2 SOBRE O PL 2793/2011, GERADOR DA LEI 12.737

O processo de aprovação da Lei nº 12.737, ou “Lei Carolina Dieckmann”, foi deveras simplificado quando comparado ao já discutido. O diploma legal originou-se do Projeto de Lei 2793/2011[12], de autoria dos Deputados Paulo Teixeira, Luiza Erundina, Manuela D’Ávila, João Arruda, Brizola Neto e Emiliano José.

O sobrecitado projeto trazia em seu bojo proposta de modificação do Código Penal (Decreto-Lei nº 2.848, de 07 de dezembro de 1940), compreendida em 04 (quatro) artigos[13]. Estava previsto o delito de invasão de dispositivo informático, no

[12] BRASIL. **PL 2793/2011**. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=529011>. Acesso em: 08 mar 2013.
[13] BRASIL. **Projeto de Lei 2793**. Disponível em: <http://www.camara.gov.br/proposicoesWeb/pop_mostraintegra?codteor=944218&filename=Tramitacao-PL2793/2011>. Acesso em: 08 mar 2013.

Art. 154-A, o qual era acrescido de 05 (cinco) parágrafos. Já o Art. 154-B estipulava que a ação seria pública condicionada à representação para os delitos citados no artigo anterior, exceto nos casos em que o crime fosse praticado contra a administração direta ou indireta e empresas concessionárias de serviços públicos.

Propunha-se, também, a inclusão dos parágrafos 1º e 2º ao Art. 266, onde passava a incorrer na mesma pena do delito de interrupção de serviço telegráfico, radiográfico e telefônico a conduta que interrompesse serviço telemático ou de informação de utilidade pública, a qual deveria ser dobrada em ocasião de calamidade pública.

Ademais, estava presente a modificação do Art. 298, para a inclusão do parágrafo único que definiria o crime de falsificação de cartão de crédito. Desta forma, o cartão de crédito ou débito seria equiparado a documento particular.

A justificativa apontada para a apresentação do PL consistia na “necessidade de regulamentação de aspectos relativos à sociedade da informação”. Segundo seus autores ele foi elaborado como opção ao Projeto de Lei 84/1999, que fora criado para esse fim, e já em avançado estado de evolução não podia sofrer modificações, muito embora estivesse destinado ao fracasso.

Segundo os elaboradores do Projeto de Lei alternativo, o PL 84/1999, era de “criminalização demasiadamente aberta, capaz de ensejar a tipificação criminalização de condutas corriqueiras, praticadas por grande parte da população na internet”.

Afirmava-se, ainda, que o intento buscado nesse rascunho opcional era a não criminalização excessiva, característica da primeira iniciativa legal, conforme o excerto: “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”

O PL 2793/2/11chegou a ser apensado e desapensado a outros esboços legislativos, sendo por fim, desengavetado após a ocorrência de um episódio que veio a batizar a futura lei. Nele, fotos da atriz Carolina Dieckmann foram retiradas de

seu computador pessoal e postadas na internet.[14] Por fim, o projeto foi levado ao Senado para votação em sua redação final, assinada pelo Dep. Nelson Peregrino[15].

O Substitutivo[16] apresentado e aprovado nesta casa provocou pequenas alterações no projeto inicial, em decorrência da modificação proposta em 05 (cinco) emendas, as quais alteravam o Art. 154-A *caput*, § 1º, § 3º, § 4º, Art. 266 *caput*, § 1º, tendo sido mantido em sua essência. A matéria foi à sanção presidencial em 08 de novembro de 2012, após a aprovação de três das cinco emendas apresentadas pelo Senado Federal.

O arcabouço legislativo foi sancionado sem vetos pela Presidenta da República, tendo sido transformada na Lei Ordinária 12.737/2012, em 30 de novembro de 2012.

3.2 AS RAZÕES QUE LEVARAM À APROVAÇÃO DAS LEIS

A necessidade de criar uma legislação que combatesse o mau uso dos meios cibernéticos foi aumentando juntamente com a abrangência destes, como já discutido.

A idéia de coibir as ações prejudiciais com as leis já existentes caiu por terra quando se percebeu que o avanço tecnológico havia criado conceitos que não mais poderiam ser interpretados pelos tipos penais existentes.

Nessa época de crescimento da dependência ao meio tecnológico, o país e suas instituições passaram a ser alvo de inúmeros ataques criminosos, os quais perturbaram a vida daqueles que necessitavam dos serviços prestados através desses meios.

---

[14] **Senado aprova Lei Carolina Dieckmann sobre crimes de internet**. Bom Dia Brasil. Disponível em: <http://g1.globo.com/bom-dia-brasil/noticia/2012/11/senado-aprova-lei-carolina-dieckmann-sobre-crimes-de-internet.html>. Acesso em: 08 mar 2013.

[15] BRASIL. **Redação Final PL 2793-A**. Disponível em: < http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=992694&filename=Tramitacao-PL+2793/2011>. Acesso em: 08 mar 2013.

[16] BRASIL. **Emendas Senado 2793/2011**. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1036167&filename=EMS+2793/2011+%3D%3E+PL+2793/2011>.

3.2.1 OCORRÊNCIAS DE ILÍCITOS CIBERNÉTICOS NO BRASIL

O Brasil tem sido alvo constante de ataques de criminosos que agem no meio cibernético, o que o tem colocado em lugar de destaque no mundo por estar dentre os locais que mais sofrem com as ações maliciosas. Ademais, o país é conhecido por ser um paraíso para os agentes promovedores dos atos ilícitos, tendo em vista o grande número de incidentes originados no território nacional.

A rápida proliferação da internet no país proporcionou em grande parte esse descontrole para com o seu uso, mesmo com a criação de instituições voltadas para a sua coordenação. Segundo Wendt e Jorge, a internet no Brasil teve início também como meio de comunicação entre universidades, tal qual o seu surgimento mundial

> [...] a primeira rede conectada à internet interligava as principais universidades brasileiras. Diferentemente da internet dos dias atuais, não existia interface gráfica. [...] Porém, no ano de 1995 passaram a disponibilizar o uso comercial da internet no país. [...]
>
> Neste mesmo ano ocorreu a criação do Comitê Gestor da Internet no Brasil (CGI – BR), com a finalidade de "coordenar e integrar todas as iniciativas de serviços de internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados". (WENDT, 2012, p. 09)

No ano de 2011, quando foi elaborada a contraproposta ao PL 84/1999 que resultou na criação da Lei 12.737/2012, o país sofreu a maior onda de ataques de *hackers* e *crackers* de sua história. [17] Os principais alvos dessas ações foram sites oficiais do governo e empresas púbicas, os quais ficaram temporariamente fora do ar para os usuários.

Dentre os atos ocorridos, o mais evidente foi praticado contra os sítios da Presidência da República e Receita Federal, em 22 de junho de 2011, quando, então, a página do órgão presidencial ficou inacessível por uma hora, das 00:40h até às 01:40h. Esse horário, conhecido por ser de acesso praticamente nulo, teve um contingente de 2 (dois) bilhões de tentativas de navegação.

---

[17] **Maior ataque hacker no Brasil partiu da Itália**. Revista Época. Disponível em: <http://revistaepoca.globo.com/Revista/Epoca/0,,EMI243559-15224,00.html>. Acesso em: 10 mar 2013

Conforme o noticiado na época, os *hackers* se utilizaram da técnica conhecida como “negação de serviço” ou DDoS (Distributed Denial of Service), baseada na sobrecarga intencional do sistema.

O ataque DDoS consiste em instalar software DDoS em máquinas invadidas e assim criar um exército de terminais manipulados, para direcioná-los contra a página vítima, como se o indivíduo infectado estivesse tentando acessá-la. Desta maneira, o provedor onde o *site* está hospedado não suporta o volume de solicitações e acaba por tornar a página indisponível, o único alento é que embora a ação cause um grande impacto, não há vazamento de informações.

Segundo o Serpro (Serviço Federal de Processamento de Dados), a ação contra o diretório da Presidência da República e Receita Federal teve origem em servidores localizados na Itália. O grupo “*LulzSecBrazil*” assumiu a autoria do ato via Twitter (microblog amplamente utilizado no mundo)[18]. Eles estariam ligados ao grupo “*LulzSec*”, vertente internacional, que anteriormente já havia invadido sítios da CIA (agência de inteligência dos E.U.A), FBI (polícia federal americana), e da empresa Sony.

Conforme Wendt e Jorge, “Esse tipo de ação pode ter uma conotação de emulação, para o autor apresentar algum destaque do grupo a que pertence, ou de ciberativista, com o intuito de defender convicções religiosas, filosóficas ou políticas.” (WENDT, 2012, p. 26)

Muitos dos ataques promovidos nessa onda foram fruto desses ditos “ciberativistas”, em uma chamada “coalizão de grupos autônomos”, quando os autodenominados *Anonymous* e *LulzSecBrazil* deflagraram aquilo que eles chamaram de operação *#AntiSec* e *#Onslaught*[19]. A primeira visava retirar do ar páginas de órgãos governamentais e a segunda trazia uma série de sites como alvo, incluindo a iniciativa privada, e encabeçando a lista estava o sítio do Superior Tribunal de Justiça.

Este não chegou a ser “derrubado”, pois fazia uso de dois servidores (espécie de computador que centraliza os pedidos de informações), no entanto, segundo os ofensores, 116 (cento e dezesseis) outros *sites* foram invadidos nessa ofensiva, ela teria sido programada quinze dias antes e executada por um conjunto de 200

[18] **@LulzSecBrazil**. Disponível em: <http://www.twitter.com/LulzSecBrazil>. Acesso em: 10 mar 2013.
[19] MARQUES, Jéferson. **Operação #AntiSec começo, meio e o fim?** Disponível em: <http://www.plantaonerd.com/blog/2011/06/24/artigo-operacao-antisec-comeco-meio-e-o-fim-moderar/>. Acesso em: 10 mar 2013.

(duzentas) pessoas. Dentre as páginas atingidas estão a da Eletrobrás, do Ministério dos Esportes, Ministério da Cultura e IBGE. Esta última foi invadida novamente por um grupo auto-intitulado *Fail Shell*[20], os quais aplicaram a chamada *defacing* (pichação virtual) ao alterar a *interface* (modo de apresentação do site), expondo um olho humano pintado de modo a fazer alusão à bandeira nacional.

Esses grupos ditos "nacionalistas" expõem a capacidade do país em ser considerado um terreno fértil para esse tipo de ação. Segundo o relatório apresentado pela *Trustwave 2013 Global Security Report*, o Brasil é o 5º (quinto) país mais representativo em atividades do cibercrime no mundo, atrás apenas dos EUA, Rússia, Taiwan e Itália, respectivamente, sendo o único país da América Latina a figurar entre os 10 (dez) primeiros.

O país também ocupa o quinto lugar dentre os países mais atingidos pela prática dos cibercrimes. Segundo o mesmo relatório, as empresas de varejo vêem sofrendo grande parte dos ataques, o que corresponderia a 45% (quarenta e cinco porcento) do total de investigações sobre violações de dados e os ataques contra o e-commerce (comércio virtual) correspondem a 48% (quarenta e oito porcento) dos incidentes reportados.[21]

Nesse sentido, outro relatório publicado pela RSA, divisão de segurança da EMC (multinacional americana de tecnologia), sobre o assunto, retratou o Brasil como um dos oito países onde mais corporações foram vítimas de fraudes virtuais em fevereiro de 2013. Muitas delas executadas através de novas modalidades da técnica utilizada por *hackers* denominada *fishing*, onde uma página da *Web* legítima é dominada por um *fisher* (algo como um *hacker-pescador*), ele transforma o sítio em uma espécie de isca, utilizada para atrair a vítima, esta quando acessa a página é redirecionada para um *site* malicioso. [22]

Desta maneira, em decorrência das fraudes, os maiores dez bancos brasileiros perderam bilhões de reais no ano anterior. Conforme estudo da consultoria *Accenture*, grande parte dos R$ 3,1 bilhões perdidos pelas instituições financeiras em 2012 foram ceifados em decorrência desses esquemas ilícitos

---

[20] **Site do IBGE permanece fora do ar após ataque de hackers.** Veja. Disponível em: <http://veja.abril.com.br/noticia/brasil/site-do-ibge-permanece>. Acesso em: 10 mar 2013.

[21] **Brasil lidera ataques cibernéticos na América Latina.** Disponível em: <http://imasters.com.br/noticia/brasil-lidera-ataques-ciberneticos-na-america-latina/>. Acesso em: 10 mar 2013.

[22] **Brasil está no TOP 5 das corporações vítimas de fraude digital**. Convergência Digital. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=33194&sid=18>. Acesso em: 10 mar 2013.

perpetrados pelos veios eletrônicos. Para evitar a repetição desses problemas, as instituições bancárias gastaram R$ 4 (quatro) bilhões de reais em medidas de proteção contra fraudes eletrônicas em 2012.[23]

Dados estatísticos divulgados pelo CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, setor vinculado ao Comitê Gestor da Internet no Brasil – CGI.br, apontaram o aumento significativo no número de incidentes reportados.

Nos últimos 13 (treze) anos, a quantidade de ações danosas no meio cibernético informadas, passaram de pouco mais de três mil em 1999, ano de criação do PL 84, para quase meio milhão no ano de 2012 (Gráfico 1), quando os primeiros diplomas voltados a criminalização dos atos ilícitos foram criados.

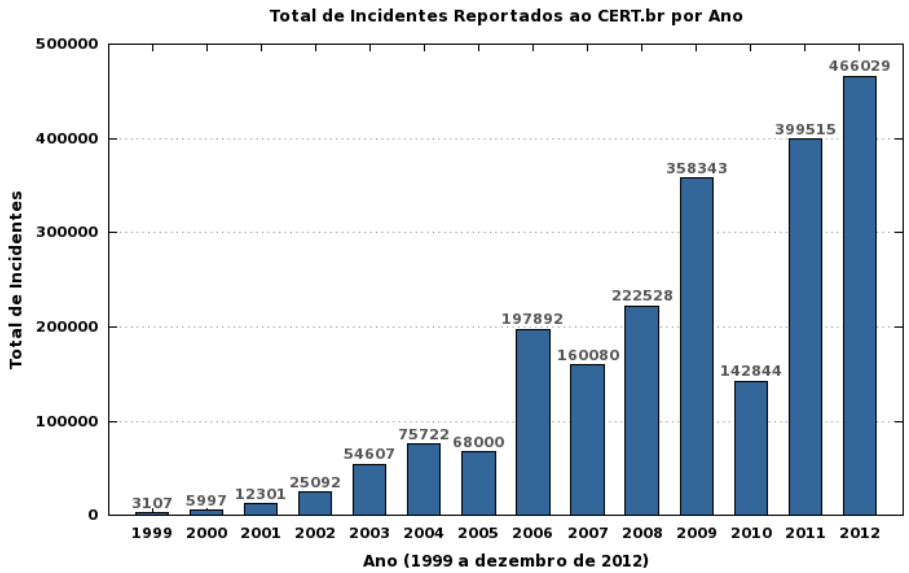

Gráfico 1 – Total de Incidentes Reportados ao CERT.br por Ano
Fonte:http://www.cert.br/stats/incidentes/#2012.

Os dados colhidos demonstraram ainda que em sua grande maioria, os ataques ocorridos em 2012 (cerca de 77, 2%), tiveram como local de origem o próprio país, seguido dos EUA (6,60%) e Canadá (4%) (Gráfico 2).

[23] **Bancos perdem R$ 3,1 bi com fraudes eletrônicas.** Exame. Diponìvel em: <http://exame.abril.com.br/tecnologia/noticias/bancos-perdem-r-3-1-bi-com-fraudes-eletronicas>. Acesso em: 10 mar 2013.

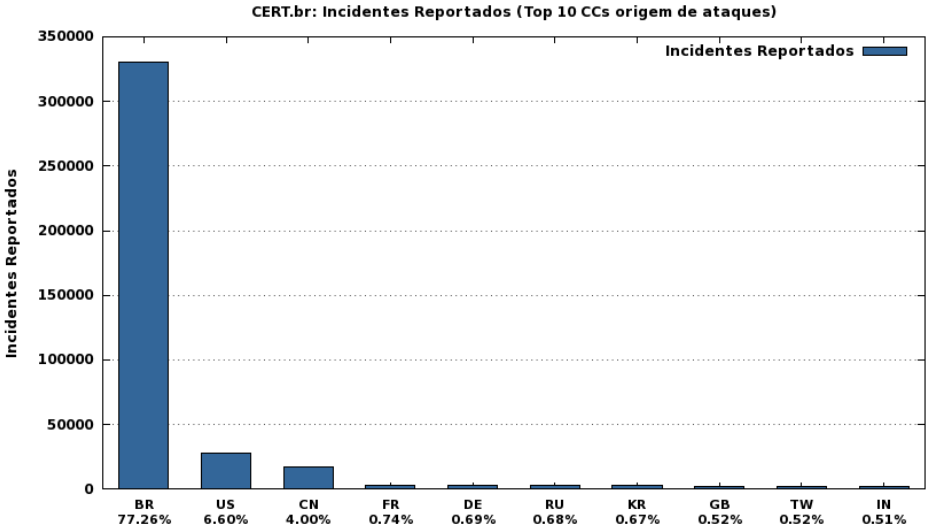

Gráfico 2 – Top 10 CCs origem de ataques
Fonte: http://www.cert.br/stats/incidentes/2012-jan-dec/top-atacantescc.html

Além disso, demonstrou-se que os maiores índices de cometimento de ações ilícitas durante a semana foram identificados de segunda a sexta-feira, de maneira que sábados e domingos representaram dias de baixa incidência de atos cibernéticos maliciosos, sendo a segunda-feira, o dia da semana em que eles são mais ativos (Gráfico 3).

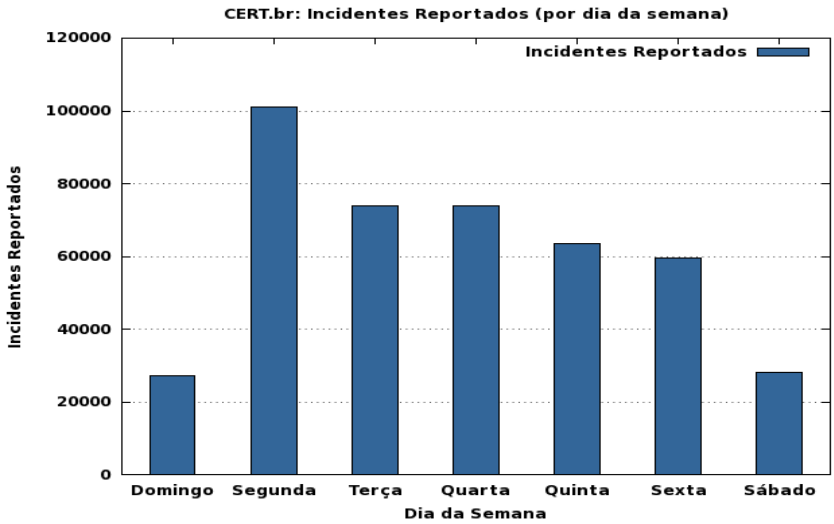

Gráfico 3 – Incidentes reportados por dia da semana.
Fonte: http://www.cert.br/stats/incidentes/2012-jan-dec/weekdays-incidentes.html

Da análise dos dados restou evidente que o mês crítico, ou seja, aquele em que tais ações foram mais intensas foi agosto, e aqueles com menor incidência foram janeiro e fevereiro (Gráfico 4).

Desta forma, traçando um paralelo com o calendário nacional é possível perceber que os meses com poucos ou sem feriados são os que apresentam maior número de ações ilícitas. É provável que isso ocorra porque o principal alvo dos atos maliciosos, empresas e instituições financeiras, estão menos tempo em funcionamento.

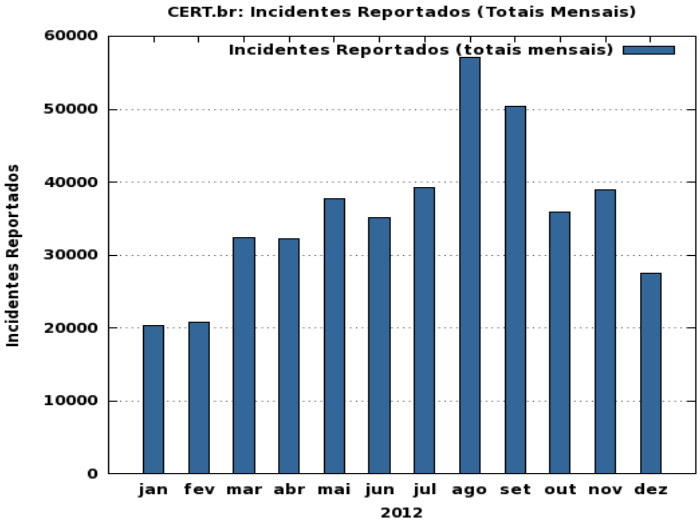

Gráfico 4 – Incidentes reportados: totais mensais
Fonte: http://www.cert.br/stats/incidentes/2012-jan-dec/ataques-mensal.html

As informações colhidas demonstraram que mais de 55% (cinquenta e cinco porcento) das tentativas de fraudes reportadas foram promovidas por meio de páginas falsas, 32,55% (trinta e dois vírgula cinquenta e cinco porcento) foram feitas através de “Cavalos de Tróia” – “que consiste em enviar um código malicioso, o qual ao ser executado compromete o computador da vítima de modo que o invasor possa tê-lo sob o seu domínio” (WENDT, 2012, 29) - e as ações contra os direitos autorais corresponderam a 6,54% (seis vírgula cinquenta e quatro porcento) (figura 5).

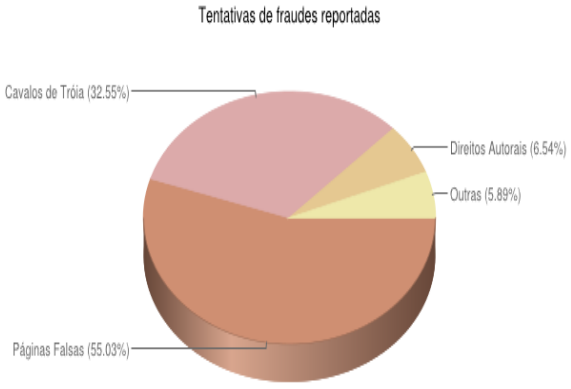

Gráfico 5 – Tentativas de fraude reportadas
Fonte: http://www.cert.br/stats/incidentes/2012-jan-dec/fraude.html

As fraudes representaram 14,93% (quatorze vírgula noventa e três porcento) das ações maliciosas reportadas, os *scans* (varreduras de dispositivos para identificar os programas presentes) 49,89% (quarenta e nove vírgula oitenta e nove porcento) e os *worms* (arquivo malicioso que se instala na memória ativa do dispositivo e possui alta capacidade de auto-reaplicação) 8,25% (oito vírgula vinte e cinco porcento) (Gráfico 6).

Gráfico 6 – Incidentes reportados: tipos de ataque
Fonte: http://www.cert.br/stats/incidentes/2012-jan-dec/fraude.html

Os dados acima atestam a percepção já apresentada aqui, ao constatar a prevalência das ações de *fishing*, como a freqüente utilização de páginas falsas, réplicas das legítimas, para atrair as vítimas e fazê-las fornecer dados sigilosos..

3.2.2 OS FATOS QUE DETERMINARAM A APROVAÇÃO DOS DIPLOMAS

O impulso inicial para criação dos diplomas repressores aqui analisados foi sem dúvida a onda de ataques às páginas de órgãos e empresas públicas, perpassada de junho a agosto de 2011, quando então, o temor sobre a insegurança dos meios cibernéticos veio à tona.

Naquele momento, as ações dos grupos de *hackers* conhecidos como "ciberativistas" reacenderam as discussões sobre a necessidade de impor limites penais às atividades no mundo virtual.

Os ataques coordenados pelos *LuIzSecBrazil* e *Anonymous* deram visibilidade a um assunto até então pouco divulgado. Na verdade, pode-se dizer que em virtude do gigantesco número de ocorrências e do campo de abrangência das vítimas, essa questão era, em muito, banalizada.

Seguiu-se então o ressurgimento das polêmicas que levaram o PL 84/1999 (89/2003) a ser conhecido como AI-5 Digital, tais quais: a acusação de promover a censura e a obrigação de retenção de *logs* ou IPs (endereço do computador na internet) por três anos pelos provedores.

Por oportuno, a bancada governista trouxe à baila um Projeto de Lei opcional (2793/2011), que segundo os seus desenvolvedores, possuía a intenção de não criminalizar o acesso à internet, mas para outros, representava apenas uma versão reduzida do PL Azeredo. [24]

Somado aos ataques, as investidas de *hackers* diretamente contra parlamentares - tal qual a invasão da página pessoal do Senador Magno Malta, quando em meio à mensagem *deface* foi chamado de homofóbico[25] - fizeram com que a exasperação por normas penais que tipificassem as ações no universo virtual ultrapassasse a idéia de votá-las em conjunto com o Marco Civil da Internet, uma nova legislação que definiria direitos e deveres dos usuários.[26]

No entanto, o que determinou a aprovação das leis foi a publicação de fotos íntimas da atriz Carolina Dieckmann. No caso em questão a conta de e-mail da vítima foi *hackeada,* de modo que os invasores tiveram acesso aos dados da vítima.

As imagens foram postadas em sites de pornografia após a atriz ter recusado a ceder à chantagem. Segundo o apurado, um dos quatro responsáveis pela ação, único menor de 18 (dezoito) anos, teria pedido a quantia de R$ 10.000,00 (dez mil

---

[24] CABRAL, Rafael. **Três projetos e duas leis.** Estadão. Disponível em: <http://blogs.estadao.com.br/link/tres-projetos-para-duas-leis/>. Acesso em: 20 mar 2013.

[25] **Senador Magno Malta denuncia à PF invasão de hackers a seu site**. Portal G1. Disponível em: <http://g1.globo.com/tecnologia/noticia/2011/06/senador-diz-que-denunciou-pf-invasao-de-hackers-seu-site.html>. Acesso em: 21 mar 2013.

[26] DIAS, Tatiana M. **Lei de crimes eletrônicos em regime de urgência.** Estadão. Disponível em: <http://blogs.estadao.com.br/link/lei-de-crimes-eletronicos-em-regime-de-urgencia/>. Acesso em: 20 mar 2013.

reais) para que as fotografias comprometedoras não fossem divulgadas.[27] Como não existiam normas que criminalizassem a invasão de dispositivo Informático alheio e o furto de dados, o fato foi caracterizado apenas como extorsão.

O caso despertou uma enorme mobilização midiática e, por conseguinte, teve muita repercussão nacional, o que trouxe aos discursos um clamor pela penalização dos ilícitos cibernéticos. A força dessa "onda" foi capaz de dar o ultimato para a votação do Projeto da Lei Azeredo e desemperrar o PL 2793/2011, o qual passou a ser conhecido como "Lei Carolina Dieckmann".[28]

Evidencia-se, aqui, mais uma vez, o poder da mídia em influenciar a produção legislativa. Ao se observar todo o processo tem-se a impressão que a privacidade de um indivíduo famoso sobressalta a segurança de órgãos e empresas públicas.

Isso pode ser entendido com a propagação das situações, pois quando da ocorrência dos atos contra os sites governamentais, apesar dos projetos de lei terem sido postos novamente em votação, acabaram por ser relegados ao tempo. Enquanto que na ocasião em que a privacidade de um indivíduo famoso foi diretamente exposta, nem a falta do marco civil da internet impediu a sua votação.

Deste modo, a exposição da intimidade de uma pessoa reconhecida foi vista e propagado como uma grande temeridade, enquanto que a onda de ataques cibernéticos ocorrida menos de um ano antes foi tratada como uma conseqüências ao uso dos dispositivos informáticos pelos órgãos oficiais, como se não significasse muita coisa.

Em que se baseiam os valores sociais de um povo que entende ser mais importante a segurança da imagem individual do que aquilo que traz um bem maior da população?

---

[27] MENEZES, Tyndaro; Soares, Paulo R. **Polícia encontra hackers que roubaram fotos de Carolina Dieckmann**. Fantástico. Disponível em: <http://g1.globo.com/fantastico/noticia/2012/05/policia-encontra-hackers-que-roubaram-fotos-de-carolina-dieckmann.html>. Acesso em: 20 mar 2013.

[28] LEMOS, Rafael. **Roubo de fotos de Carolina Dieckmann acelera tramitação de projeto de lei sobre crimes cibernéticos**. Veja. Disponível em: <http://veja.abril.com.br/noticia/brasil/roubo-de-fotos-de-carolina-dieckmann-acelera-tramitacao-de-projeto-de-lei-sobre-crimes-ciberneticos>. Acesso em: 20 mar 2013.

4. UMA ANÁLISE DOS NOVOS DIPLOMAS LEGAIS

4.1 A LEI 12.735 DE 30 DE NOVEMBRO DE 2012

A Lei sancionada em 30 de novembro de 2012 pela Presidenta da República possui a seguinte ementa:

> 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.

A Lei, inicialmente pensada para ser extravagante, foi alterada para que seus artigos fizessem parte dos diplomas penais já existentes. Essa integração dos novos tipos penais ao ordenamento muito simboliza o pensamento inicial sobre as punições dos crimes cibernéticos, o qual apontava que tais delitos poderiam ser combatidos apenas com a legislação penal existente.

Embora afastada, a idéia de que os bens da vida maculados pelos ilícitos cibernéticos poderiam ser protegidos pelos tipos penais previstos na década de 1940, ano de criação do atual Código Penal, influenciou na elaboração do presente trabalho legislativo.

A opção do legislador por alterar a Lei 7.716/1989 e os Códigos Penal e Militar, demonstra, ainda, a intenção de não criar tipos penais que pudessem ser vistos como algo distante da realidade. Ou até de prevenir uma possível ineficácia da Lei, fenômeno comum no país, e que ocorre quando ela existe, mas não é aplicada.

A possibilidade de que a apresentação das novas figuras penais causasse tais impressões era muito presente, principalmente levando-se em conta o estado de banalização das ilicitudes, em muito provocado pelo vasto número de vítimas. Isso

criava a impressão de normalidade, como se ter o computador invadido fosse uma consequência para quem o utilizava, esse seria o ônus da tecnologia.

Outra coisa que se buscou afastar com a alteração normativa, foi o tecnicismo, já que este também poderia refletir em falta de efetividade da norma. A existência desta em uma lei separada poderia dar a entender que ela não estava voltada para todos que utilizam os meios cibernéticos, mas apenas para aqueles que o entendem em sua essência e com ele interagem com facilidade, tais quais os temidos *hackers* e *crackers.*

O trabalho legislativo teve como escopo "tipificar condutas realizadas mediante o uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares."

De início, faz-se necessário entender o que vem a ser um sistema eletrônico, digital ou similar. Segundo o Dicionário Aurélio (FERREIRA, 2004), "um sistema constitui-se em partes ou elementos de um todo que coordenados entre si, funcionam de modo organizado."

Já o termo "eletrônico", vem de eletrônica, ciência definida como estudo de circuitos formados por componentes elétricos e eletrônicos, os quais existem com o objetivo de transformar, transmitir, processar e armazenar energia[29]. Desta maneira, os instrumentos eletrônicos armazenam e transmitem dados.

Nesse caminho, o sistema digital também se constitui em um braço da eletrônica, porém, a despeito de utilizar a energia elétrica para emitir sinais e assim transmitir e armazenar informações, isso é feito de uma forma diferente. Os circuitos digitais fazem uso dos sinais em dois níveis de corrente ou tensão elétrica, as quais representam valores distintos em um sistema binário.

Esse sistema é baseado na transmissão de dados expressos apenas com a combinação de seqüências de dois dígitos, o "0" e o "1". Somente com os dois símbolos numéricos, as informações são transmitidas, armazenados, descartados, criados ou de qualquer forma modificados. É a essencialidade dos dois dígitos para a existência do sistema que o nomeia de "digital".[30]

A lei também se destina às condutas praticadas mediante uso de sistemas similares ao eletrônico e digital. O que leva a entender que estes ou outros

---

[29] **ELETRÔNICA**. Wikipédia. Disponível em: <http://pt.m.wikipedia.org/wiki/Eletr%C3%B4nica> Acesso em: 24 de mar 2013.

[30] **CIRCUITO DIGITAL**. Wikipédia. Disponível em: <http:// pt.m.wikipedia.org/wiki/Sistema_digital>. Acesso em: 24 mar 2013.

elementos coordenados, tenham como base os princípios de funcionamento que caracterizam os sistemas já descritos.

Essas condutas a serem combatidas são aquelas praticadas contra sistema informático e similares, ou seja, elementos coordenados através da análise numérica, que trabalham em conjunto na transmissão, armazenamento e demais movimentação de informações em meio eletrônico, seguindo processos automáticos em sistemas binários.

Mas uma vez o legislador confunde o objeto material da norma com o bem juridicamente protegido, vez que determina que as normas descritas nesta lei, visam tipificar os atos praticados por meio de sistema eletrônico, digital ou similares, contra sistema informático.

Ora, pois, os sistemas informáticos também compreendem uma faceta da ciência eletrônica e são em sua essência digitais. Observa-se aqui, claramente, a ausência da técnica na elaboração da norma penal, de maneira que o bem juridicamente protegido, nesse caso as informações manipuladas por esses sistemas, se quer é citado, e acaba por ser confundido com o principal ramo da ciência especializada na propagação de informações.

4.1.1 CONSIDERAÇÕES SOBRE OS ARTIGOS 1º AO 5º

A presente lei, inicialmente pensada para tipificar delitos de informática foi reduzida, a poucos artigos, não trazendo nenhuma figura de delitos informáticos próprios. Assim acabou por servir de sustentáculo para o projeto apresentado como alternativo. Contudo, a sua análise se faz necessária, pois foi no bojo desse projeto que a maior parte das discussões sobre a criação dos delitos cibernéticos ocorreu.

> **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.

O art. 1º e a ementa que apresenta a norma penal são os mesmos, de maneira que as considerações iniciais já apresentadas aqui dão a dimensão que a Lei é dirigida.

O diploma legislativo prevê a tipificação de condutas, de modo a formalizar a existência de delitos até então entendidos apenas como condutas ilícitas, tendo em vista que não podiam ser reprimidos através das normas anteriormente existentes. Para tanto, descreve o seu foco de ação, a que se destina e o que vai atingir com seus dispositivos.

Art. 2º (VETADO)

O artigo 2º foi vetado pela Presidenta da República quando da sanção da Lei. Tratava-se da tipificação do delito de falsificação de cartão de crédito, o que incluiria um parágrafo único no Art. 298 do Código Penal, o qual regula os crimes de falsificação de documento particular.

Nesse sentido o cartão de crédito ou débito seria equiparado a essa modalidade de documento. No entanto, como a conduta a ser condenada já fazia parte dos ilícitos tipificados na Lei 12.737/2012, aprovada em conjunto com esta, o artigo foi vetado com a justificativa de que o delito lá descrito possuía *nomem juris* mais adequado, como também esta seria uma forma de evitar uma duplicidade desnecessária.

Tal fato serve de apoio para aqueles que entendiam que o Projeto de Lei alternativo apresentado pela base governista, o qual veio a sagrar-se no diploma legal sobrecitado, compunha-se, em verdade, de um resumo dos artigos existentes no rascunho inicial do PL 84/1999, transformado neste diploma legislativo.

Art. 3º (VETADO)

Os dois incisos previstos no Art. 3º modificariam o delito de favor ao inimigo, existente ao Art. 356 do Código Penal Militar. De modo que incluiria aos incisos já existentes II e III o termo “dado eletrônico”, desta maneira eles passariam a ter as seguintes redações:

> Favor ao inimigo
>
> Art. 356. Favorecer ou tentar o nacional favorecer o inimigo, prejudicar ou tentar prejudicar o bom êxito das operações militares, comprometer ou tentar comprometer a eficiência militar:
> I - ...
> 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;
> IV - ...
> V - ...
> Pena - morte, grau máximo; reclusão, de vinte anos, grau mínimo. (grifo nosso)

A razão para o veto foi apoiada na amplitude do conceito de dado eletrônico. Isso impossibilitaria a aplicação da norma, pois seria sobremodo difícil determinar em que situação ele se enquadraria, tendo em vista que se trata de um nome genérico para qualquer fluxo de impulsos elétricos em meio eletrônico que podem ou não significar uma informação relevante.

Seguindo essa linha de raciocínio, o dado eletrônico corresponderia a toda informação transmitida por meio da ciência eletrônica, o que poderia ser entendido como qualquer coisa que passasse por esse tipo de equipamento e chegasse ao inimigo da nação ou pudesse contribuir para o prejuízo das ações militares do país.

Ainda de acordo com esse entendimento, a inclusão do citado objeto material nos respectivos incisos, criaria normas penais em branco, tendo em vista, a já explanada dificuldade de determinação do conceito de dado eletrônico.

No entender do Mestre e Doutor Rogério Greco, norma penal em branco consiste:

> Diz-se em branco a norma penal porque seu preceito primário não é completo. Para que se consiga compreender o âmbito de sua aplicação é preciso que ele seja complementado por outro diploma, ou, na definição de Assis Toledo, normas penais em branco “são aquelas que estabelecem a cominação penal, ou seja, a sanção penal, mas remetem a complementação da descrição da conduta proibida para outras normas legais, regulamentares ou administrativas.” (GRECO, 2010, p. 64 Apud TOLEDO)

Desta feita, podemos entender que inserção de um termo com interpretação tão vasta, poderia determinar a necessidade de delimitação do seu significado.

> **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.

Tal norma visa a criação de setores especializa na investigação de delitos cibernéticos, vez que tais crimes possuem meios de prova distintos dos habituais, tendo em vista que os fatos ocorrem em ambiente virtual, não palpável, o que diferencia a materialidade dos delitos.

A atividade desses órgãos especiais vai promover a fase investigativa, pré-processual ou administrativa, voltada para a coleta de vestígios e evidências que venham a basear a ação penal em um futuro próximo.

Segundo Aury Lopes Jr, “Não se deve começar um processo penal de forma imediata. Em primeiro lugar, deve-se preparar, investigar e reunir elementos que justifiquem o processo ou não-processo.” (LOPES JUNIOR, 2010, p. 224)

Os meios digitais possuem como característica a efemeridade na guarda das informações, visto que tais não são resguardadas de forma física. A volatilidade com que elas são armazenadas e logo depois apagadas constitui o grande e provavelmente, maior impedimento às investigações criminais.

Os dados são armazenados em dispositivos magnéticos, de modo que podem ser apagados quando são formatados, ou seja, quando os caminhos para a localização dos arquivos no disco são desfeitos.

Outrossim, a maior parte das ações investigativas têm início com a localização dos computadores ou outros dispositivos informáticos, de onde os comandos para os atos delituosos tiveram início. E para isso é preciso que se descubram os *logs* ou IPs (endereços dos processadores na internet), o que demanda técnica, além da ajuda dos provedores. (COLLI, 2010, p. 117)

No atual estágio de desenvolvimento tecnológico que as sociedades modernas se encontram, os dados passam a ser armazenados na chamada “nuvem”, um servidor remoto, que pode estar em outro país ou continente. De modo que, aqueles que a utilizam necessitam apenas de uma conexão com a internet para terem acesso a eles.

Isso dificulta a identificação dos autores dos fatos, posto que a evidência capaz de atesta os crimes não pode ser encontrada com que os pratica, porém

estes podem acessar seu sistema ou programa malicioso de qualquer lugar do globo. (WENDT et al, 2012, p. 179)

Por tudo isso, e pela constante transformação dos métodos utilizados na consecução dos atos ilícitos, faz-se necessário tanto um aparato quanto um corpo técnico especializado nas características desses objetos, para que desta forma as evidências sejam coletadas.

> **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)

Tal artigo faz modificações na §3º do Art. 20 da Lei que define crimes resultantes de preconceito de raça ou de cor. O que sinaliza a utilização dos dispositivos cibernéticos também na efetivação dos crimes dessa natureza.

Aqui os mecanismos eletrônicos servem como instrumento, de modo que o delito não se exaure nele, são os conhecidos delitos informáticos (como sinônimo de cibernético) impróprios. A intenção é impedir que as novas tecnologias sirvam como forma de disseminação da intolerância racial, como já é feito em por outros meios de comunicação.

> **Art. 6º** Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.

A *vacatio legis* estipulada para que a norma entrasse em vigor foi de 120 (cento e vinte) dias a contar da sua publicação oficial. Tal período serviu principalmente como tempo necessário a estruturação das delegacias e demais órgãos especializados na investigação desse tipo de delito, as quais tiveram sua criação determinada no Art. 4º desta Lei.

Como a norma foi publicada no Diário Oficial da União em 03 de dezembro de 2012, esta passou a vigorar em 02 de abril de 2013. Aplica-se aqui a norma do Art. 10 do Código Penal, onde o dia do início do prazo é computado na contagem deste.

4.2 ANÁLISE DA LEI 12.737/2012 (Lei Carolina Dieckmann)

A ementa que faz a apresentação deste diploma normativo ressalta a sua funcionalidade nos seguintes termos:

> 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.

Tal qual a Lei Azeredo (Lei nº 12.735/2012), o presente diploma legal faz modificações no Código Penal, de modo que aqui também se buscou manter a idéia de que os delitos cibernéticos não se afastam sobremaneira da realidade material, podendo ser reprimidos com a aplicação da legislação já existente.

Ademais, a introdução dos novos tipos no diploma codificado fortalece o ideal de unicidade e combatibilidade da legislação penal, já desgastado com a disseminação de normas criminais em legislações relativas a assuntos diversos.

4.2.1 CONSIDERAÇÕES SOBRE OS ARTIGOS 1º E 2º

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

A descrição da Lei como tipificação criminal dos delitos Informáticos feita aqui, vem a englobar os cibercrimes. Neste caso, o termo “informáticos” pode ser interpretado pela hermenêutica jurídica como sinônimo de cibernéticos, tal como ocorre na literatura especializada.

Isso ocorre, como já visto no início desse trabalho, em razão da ciência cibernética desenvolver-se no sentido da informática, baseada na transferência de dados através da eletrônica e da coordenação desses por fórmulas e funções matemáticas.

Segundo um dos estudiosos no assunto, o Prof. Maciel Colli, isso pode ser explicado pela ligação entre eles:

> A ligação entre cibernética, ciberespaço e crimes informáticos permite que se compreenda o instituto do cibercrime como sendo aquele no qual um ou mais computador(es), equipamentos telemáticos ou dispositivos eletrônicos, interligados por meio de uma rede de comunicação, são utilizados por um mais indivíduos, no cometimento de uma ou mais, conduta(s), criminalizada(s), ou são alvo(s) desta(s). (COLLI, 2010, p. 44)

Sendo assim, podemos entender que os tais sistemas informáticos, por estarem inseridos no ciberespaço pode ser entendido como um sistema cibernético.

> **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.

O *caput* do presente artigo pode ser considerado o maior avanço proporcionado pela criação de normas que reprimem os delitos cibernéticos. Tem-se em conta que ele veio combater as principais práticas danosas conhecidas por causarem transtornos aqueles que utilizam ou de alguma forma dependem dessas tecnologias.

O novo artigo tem como intenção combater a invasão de dispositivo informático alheio, conectado ao não a rede de computadores. Nesse ínterim, criminaliza-se a invasão, ou seja, o acesso sem permissão ao conteúdo armazenado em dispositivo informático (aqui como sinônimo de cibernético) estando este ou não conectado à rede de computadores.

A Lei prevê que tal ação ilícita seja realizada mediante a violação de mecanismo de segurança, o que na maioria das situações significa um sistema anti-vírus, utilizado para proteger o meio tecnológico das ameaças sistêmicas como *cavalo de troia*, *spans* e principalmente os vírus de computador. Mas também pode corresponder a obrigação de preencher senhas de acesso aos sistemas, bancos de dados, páginas e demais funções presentes nos aparelhos informáticos.

Essa questão significa para muitos a maior falha da Lei. A ressalva existente no *caput* do artigo acaba por condicionar a invasão do dispositivo a uma violação de mecanismo de segurança.

Fazendo uma comparação com o delito de violação de domicílio, existente no Art. 150 do Código Penal, este crime só ocorreria se o indivíduo adentrasse ao recinto após ultrapassar de algum modo as barreiras que o impediriam de entrar simplesmente, tal qual uma porta trancada.

Assim, seguindo o raciocínio da norma aqui posta, se a entrada do agente não ocorresse da maneira citada, como no caso deste aproveitar a porta aberta, o delito não existiria.

A comparação com o crime de violação de domicílio vem a calhar aqui, pois podemos imaginar que de certa forma tais mecanismos cibernéticos funcionam como domicílios para o perfil do indivíduo, o "eu virtual" dos seus donos, tendo em vista que guardam suas características e dados íntimos.

Em seu artigo, o Professor e também Delegado de Polícia Eduardo Cabette destaca o despropósito da situação condicionada, vejamos:

> Sinceramente não se compreende essa desproteção legislativa exatamente aos mais desprotegidos. É como se o legislador considerasse não haver violação de domicílio se alguém invadisse uma casa que estive com as portas abertas e ali permanecesse sem a autorização do morador e mesmo contra a sua vontade expressa! Não parece justo nem racional presumir que quem não instala proteções em seu computador está permitindo tacitamente uma invasão, assim como deixar a porta ou o portão de casa abertos ou destrancados não significa de modo algum que se pretenda permitir a entrada de qualquer pessoa em sua moradia. (CABETTE, 2013)[31]

A necessidade de existência de um mecanismo de segurança e ainda de burlá-lo para a caracterização do crime, divide especialistas. Muito embora, a maioria entenda que a simples solicitação de uma senha de acesso seja suficiente para atestar a existência de um dispositivo de proteção.

Por esse caminho, não só o método para promover a segurança deve existir, como também deve estar apto a promovê-la, o que significa em muitos casos não só a instalação dessas medidas, como também a sua atualização.

---

[31] CABETTE, Eduardo L. S. **O novo crime de Invasão de Dispositivo Informático**. Consultor Jurídico. Artigo publicado em 4 de fev 2013. Disponível em: <http://www.conjur.com.br/2013-fev-04/eduardo-cabette-crime-invasao-dispositivo-informatico>. Acesso em: 25 de mar 2013.

Os principais métodos utilizados hoje, ou seja, os anti-vírus, funcionam com esse princípio. Necessitam, estar sempre sincronizados com as novas técnicas utilizadas no combate as ameaças do meio eletrônico, só assim podem funcionar impedindo o acesso destas.

Também na opinião do Professor Eduardo Cabette, isso pode ser considerado um despropósito. Leia-se:

> Observe-se ainda que ao exigir a "violação indevida de mecanismo de segurança", não bastará a existência de instalação desses mecanismos no dispositivo informático invadido, mas também será necessário que esses mecanismos estejam atuantes no momento da invasão, caso contrário não terá havido sua violação e o fato também será atípico, o que é ainda mais estranho. (CABETTE, 2013)[31]

O tipo penal trabalha com o núcleo baseado no verbo invadir, este tem o sentido de entrar sem a permissão devida, ter acesso a local que não deveria, entrar à força, tendo em vista a já citada necessidade de violação da segurança. Ou seja, invadir nesse caso, é passar por barreiras que impediriam o simples acesso ao sistema informático sem estar autorizado por quem é de direito.

Segundo o *caput* do artigo a necessária autorização do titular do dispositivo pode ser expressa ou tácita. A permissão dada por ele, no entanto, não o limita como vítima, se dentre os dados ou informações adulterados, obtidos ou destruídos existir os de outros indivíduos estes também serão considerados como agentes passivos da ação.

4.2.2 CARACTERÍSTICAS DO DELITO

O delito aqui analisado é comum quanto ao sujeito ativo e passivo, podendo ser praticado por qualquer pessoa e sofrido da mesma forma por qualquer um, o que significa que não é preciso nenhuma qualidade especial para praticá-lo, tanto do sujeito ativo como passivo.

Crime doloso, comissivo, formal, não é necessário que o invasor venha a obter de fato os dados preteridos ou instale vulnerabilidade, instantâneo ou

permanente, monossubjetivo, plurissubsistente (admite tentativa), simples e não transeunte.

Como já vimos anteriormente, o objeto material do tipo é o dispositivo informático, o que aqui pode significar de uma memória *pen drive* a um banco de dados de um servidor. Basta somente que eles utilizem ou estejam baseados na tecnologia telemática.

O delito está por sua vez inserido no capítulo VI que trata dos crimes praticados contra a liberdade individual, ainda dentre a seção IV, que regula os ilícitos contra a inviolabilidade dos segredos. Deste outro modo, resta clara a intenção do legislador de resguardar a liberdade e privacidade dos usuários desses sistemas, o que sinaliza que este também é um bem que veio a ser protegido com o novo diploma legal.

A conduta tipificada no *caput* do Art. 154-A pode ser praticada por qualquer um, como já dito aqui, não é preciso qualquer qualidade especial para intentá-la o que o caracteriza como crime comum.

Da mesma forma, qualquer pessoa, seja ela nesse caso física ou jurídica, pode ser alvo, sujeito passivo do crime, o que o torna comum, também por esse viés.

> **§ 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.

O parágrafo primeiro determina a aplicação da pena prevista para o delito de invasão de dispositivo informático em 3 (três) meses a 1 (um) ano de detenção, para aqueles que produzam, distribuam, vendam ou difundam dispositivo ou programa de computador voltado para a prática da conduta descrita como crime no *caput* do artigo.

Intenta-se assim, evitar que os meios ou instrumentos utilizados em tais ações sejam disponibilizados para aqueles que poderiam fazer o mau uso deles. Desta forma, a menor oferta destas ferramentas teria o condão de diminuir a ocorrência dos fatos ilícitos.

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

Tal medida visa principalmente à proteção daqueles que utilizam os meios informáticos na consecução de negócios, como bancos e empresas. No entanto, dado o avanço significativo da tecnologia da informação voltada ao comércio eletrônico, atividade muito visada por aqueles que promovem tais atos ilícitos, qualquer cidadão pode vir a sofrer um prejuízo econômico significativo.

O atual e cada vez mais difundido modo de pagamento eletrônico, faz com que os usuários disponibilizem dados relativos às suas contas bancárias e cartões de crédito no meio no sistema informático. Em fim, o citado aumento possui o condão de inibir as fraudes eletrônicas, uma das questões mais graves do mau uso dos sistemas informáticos.

> **§ 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.

O legislador optou por majorar a pena para os casos em que as conseqüências da invasão, a seu ver, podem ser entendidas como a descoberta de dados que o titular não tinha o interesse de divulgar. Desta forma, ele listou aquelas situações mais conhecidas por trazer maiores aborrecimentos a quem as sofre.

Desta forma, o caput do Artigo seria uma espécie de crime meio, e em ocorrendo as conseqüências, ou o fim especial a que as ações ilícitas iniciais deram cunho a pena seria aumentada.

Nessa listagem está o conteúdo de comunicações eletrônicas, o que engloba a comunicação escrita, falada ou gravada em vídeo, tal quais as teleconferências. Estão presentes ainda, os segredos comerciais ou industriais, sempre visados como a segurança restrita.

Incluem-se também as informações sigilosas, as quais devem ser definidas em lei e o controle remoto não autorizado. Esse ponto causa maior divergência, visto que não há entendimento de como a autorização para que alguém controle o dispositivo a distância deve ser feita, pois a permissão pode ser dada por um leigo em informática sem que este saiba, através de alguns programas que habilitam tal ação de forma automática.

A pena prevista nestes casos específicos é o dobro daquela apresentada no *caput* do artigo, podendo compreender 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.

Mais uma vez o legislador prevê penas maiores para aquelas situações que possam tornar a prática do delito mais danosa à vítima. Nesse caso a propagação das informações obtidas de modo ilícito pode ser considerada a pior consequência para os seus titulares. E para inibir a ocorrência dessas conseqüências nocivas aplica-se a majoração.

> **§ 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."

Nos casos em que tais figuras representativas da nação forem afetadas por tais ações ilícitas, seja do tipo previsto no *caput* do artigo ou da sua forma qualificada a pena é aumentada

> 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.

O presente artigo traz a identificação da ação penal como pública condicionada à representação, desta maneira, para que haja a persecução penal faz-se necessário que a vítima apresente o pedido perante a autoridade pública.

Já nos casos em que o delito for cometido contra a administração pública direta ou indireta de qualquer dos poderes da União, Estados, Distrito Federal e Municípios, ou concessionária de serviços públicos, a ação passa a ser pública incondicionada. Ou seja, não necessita de provocação que a ação penal seja iniciada.

Uma questão a que se deve dar atenção é a possibilidade de o delito informático próprio ocorrer como crime meio, propiciando a existência de um delito fim que terá seus efeitos no mundo material. A dúvida aqui presente remete ao que deve ser levado em conta, se os dois delitos, em uma das modalidades do concurso de crimes, ou se apenas o delito fim, com a aplicação do princípio da consunção.

Embora não haja entendimento jurisprudencial sobre o assunto, ante o pouco tempo que a norma está em vigor, o pensamento doutrinário, o qual também é esboçado aqui, não faz distinção do universo de ocorrência do crime meio, de maneira a interpretar que o ilícito fim absorve o delito meio.

O princípio da consunção é baseado no afastamento de uma figura típica que já esteja englobada em outra. É definido por Mirabete como “O princípio da consunção (ou absorção) consiste na anulação da norma que já está contida em outra; ou seja, na aplicação da lei de âmbito maior, mais gravemente apenada, desprezando-se a outra, de âmbito menor.”

Com relação aos delitos informáticos, deve-se atentar a dependência entre eles, se a existência da última ação que terá seu fim no universo material não estiver condicionada a ocorrência da primeira os delitos serão independentes e desta maneira poderão ser considerados em separado.

Cabette ressalta a natureza do delito de invasão de dispositivo informático de modo a chamar a atenção para esse aspecto, vejamos:

> É preciso estar atento para o fato de que o crime previsto no artigo 154 – A, CP pode ser meio para a prática de infrações mais graves, tais como estelionatos, furtos mediante fraude, dentre outros. Nesses casos, seja pela subsidiariedade, no caso do artigo 154 – A, § 3º, CP, seja pela consunção nos demais casos, deverá haver prevalência do crime–fim e afastamento do concurso formal ou material com o crime de “Invasão de Dispositivo Informático”. (CABETTE, 2013)

Nesse ínterim, o delito fim que teve sua ocorrência propiciada pelo crime cibernético meio, passa a perfazer a classe dos delitos informáticos mediatos ou indiretos como se ele tivesse herdado essa característica do outro.[32]

4.2.3 CONSIDERAÇÕES SOBRE O ART. 3º

> **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)

O Art. 3º da “Lei Carolina Dieckmann” altera o delito tipificado no Art. 266 do Código Penal incluindo na descrição do tipo o serviço informático, telemático ou de informação de utilidade pública. Assim, não só a interrupção de serviço telefônico, mas das demais formas de comunicações atuais passa a ser crime. Uma atualização necessária as transformações da tecnologia da informação.

Ocorre que a pena determinada para quem pratica o delito contido no §1º não foi especificada, de modo que a que estava em vigor não mais existe. Assim, a pena de aplicação é a do Art. 265. Além disso, manteve-se o parágrafo único do artigo agora na forma do §2º.

> 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)

---

[32] MIRANDA, Murilo. **Da persecução penal dos crimes virtuais**. Jus Way: sistema educacional online. Publicado em 27 de janeiro de 2013. Disponível em: < http://www.jurisway.org.br/v2/dhall.asp?id_dh=9903>. Acesso em: 17 de abr 2013.

O referido parágrafo único faz a equiparação entre o cartão de crédito ou débito com o documento particular. Essa era uma questão antiga, muito discutida, e já estava presente no Projeto de Lei 84/1999.

Antes dessa mudança, a falsificação de cartão de crédito só poderia ser punida com a utilização deste, na forma do delito de estelionato Art. 171 do Código Penal, tendo em vista a vantagem ilícita obtida no momento em que as operações de crédito eram realizadas. Desta feita, a clonagem do dispositivo magnético em nada representava para a lei.

A inclusão do delito de falsificação de cartão de crédito no Art. 298 foi realizada com o objetivo de proteger a fé pública, e principalmente de tranqüilizar o lesado. Ocorrendo a duplicação do instrumento de crédito e em seguida o seu uso, o falso tenderá a ser absorvido pelo delito de estelionato, tendo em vista o princípio da consunção e a Súmula nº 17 do STJ.

5. AS PERSPECTIVAS DIANTE DA APROVAÇÃO DAS LEIS E O QUE MUDA NA PRÁTICA COM OS NOVOS DIPLOMAS

A criação dos diplomas legislativos aqui analisados teve o condão de preencher o vazio normativo existente na legislação penal brasileira, o qual permitia a prática de atos nitidamente ilícitos, ante a ausência de tipificação normativa.

Desta feita, intentou-se coibir as ações que maculavam a utilização dos meios cibernéticos, de modo que fossem criadas novas figuras capazes de reprimir os atos nocivos mais praticados.

Desejou-se com isso cumprir os princípios que norteiam o Direito Penal Pátrio. Dentre eles, o da legalidade em sua faceta que determina a existência previa da lei em relação ao fato ocorrido – *nullum crimen nulla poena sine lege praevia.*

Também foi levada em consideração a determinação para a criação de tipos penais apenas através da lei escrita – *nullum crimen nulla poena sine lege scripta*. E principalmente a proibição da analogia *in mallam partem*, o que indica que ela nunca pode ser utilizada na lei penal nos casos em que represente uma piora para o réu, o que vem a significar aqui, que ela não pode ser usada para criminalizar condutas que se exaurem no universo virtual por estas serem semelhantes às praticadas no mundo material.

Sendo assim, espera-se com a aprovação das normas, que o país deixe de ser considerado um local livre para a prática desse tipo de ação, em especial para as figuras dos *hackers* e *crakers.* Com isso, busca-se também que o Brasil deixe de ser um dos países que mais sofre com os ataques cibernéticos e que da mesma maneira, mais o promovem.

A segurança da informação, de fato, foi o foco das novas normas. Nesse ínterim, é desejo de todos que haja maior proteção à intimidade e liberdade individual com o resguardo dos dados pessoais disponibilizados em dispositivos informáticos.

Intenta-se sobremodo, que a utilização dos mecanismos cibernéticos possa ser considerada segura. De maneira que seus usuários não fiquem receosos ao disponibilizarem suas informações nesse meio.

Nessa esteira, casos como o da atriz Carolina Dieckmann, ocorrido em razão do “furto” de imagens íntimas dela, após invasão de seu computador pessoal, poderão agora ser entendidos como crime. De maneira que não será necessário, como antes, que o fato deságüe em outro delito para ser reprimido.

Outra questão importante é que não só quem pratica a ação de invadir dispositivo informático alheio, mas também que cria as ferramentas para isso (no caso, os programadores e etc.) poderão ser punidos com base na equiparação destes com os invasores, prevista na Lei em seu §1º do Art. 154-A.

A Lei resguardou ainda as figuras que representam o poder estatal. De maneira que esses delitos praticados contra elas, ensejam um aumento na pena a ser aplicada.

Ademais, agora, a interrupção do serviço informático, telemático ou de informação de utilidade pública, termos incluídos no Art. 266, constitui crime. Uma atualização necessária a modernidade, visto que, há tempos o telefone não é o único meio de comunicação utilizado pelos brasileiros.

De outro modo, ataques cibernéticos que deixem páginas da internet fora do ar, tais quais os baseados na tecnologia DDoS, aqui citada, poderão ser punidos. Muda também a questão dos cartões de crédito ou débito, a ação de falsificá-los já constitui crime. Assim, indivíduos responsáveis pela criação deles, poderão responder pelo delito mesmo que não tenham usufruído do crédito da vítima.

Para o cidadão comum a lei não altera muita coisa. Esse vai continuar fazendo uso dos dispositivos informáticos, quase como antes. Contudo, a tipificação do delito de invasão de dispositivo informático criou para os seus usuários a obrigação de ter um sistema de segurança, e mais, de mantê-lo atualizado.

Ainda em decorrência da criação do tipo penal, alguns setores que trabalham com essas tecnologias, tais quais os técnicos em manutenção, deverão adequar-se, para evitar que suas ações não venham de encontro à lei. Sendo assim, a necessária de autorização do titular do dispositivo para que outro alguém tenha acesso ao conteúdo nele armazenado, não pode ser esquecida.

Isso traz um problema também para aqueles que criam programas especializados em burlar sistemas de segurança, muitas vezes utilizados na reparação destes. Ainda será preciso que haja uma distinção destes para aqueles que inventam os conhecidos programas maliciosos.

Mas o que muda significativamente é a forma de combate a esses crimes. Agora, setores especializados da polícia judiciária serão responsáveis pela investigação dos delitos, o que deve facilitar na hora de desfazer a principal característica destes, o anonimato, e que tira das vítimas a obrigação de recolher evidências, o que ocorria até então.

6. CONCLUSÃO

Chegamos ao fim deste trabalho após termos abordado o mundo do cibercrime e analisado as tentativas de minimizar a sua ocorrência.

Podemos observar que o universo cibernético está incluso no dia-a-dia das sociedades modernas, de maneira que não se trata de ficção científica do nosso viver. Cada vez mais associado a uma imagem ou reprodução digitalizada.

Vive-se hoje mais de uma vida, pois além da existência física há ainda os inúmeros perfis virtuais. Podemos dizer que somos dependentes da tecnologia lógica, sem a qual não fazemos maior coisa.

Procuramos proteger aquilo que entendemos ser importante na vida e, para tanto queremos, a certeza dos processos mecânicos. Porém, não estamos livres daqueles que conseguem transformar a segurança dos processos lógicos em instabilidade e falta de confiança, diante de situações criadas para prejudicar os usuários desses sistemas.

Como foi visto, o desenvolvimento tecnológico propiciou novas formas de praticar antigos delitos, como também fez nascer novos valores, estes atrelados ao convívio cotidiano com os dispositivos informáticos (aqui como sinônimo de cibernético).

Assim, verificou-se a ocorrência dos ilícitos informáticos propriamente ditos, os quais ocorrem quando a ação maculante tem início e fim no meio virtual, sem que sua consumação chegue ao mundo material, muito embora seus reflexos o alcancem.

Tais feitos não podiam ser reprimidos com a legislação penal existente, datada de 1940, de maneira que era preciso que houvesse a criação de novos tipos penais capazes de criminalizar essas condutas. Sem isso, era necessário que as ações ilícitas causassem algum efeito reconhecido pelas normas penais vigentes. Só assim, o combate criminal poderia ocorrer.

Essa situação foi agravada com a crescente dependência da sociedade brasileira dos mecanismos tecnológicos, o que fez aumentar o número de vítimas de tais ações. Por conta disso, foram propostos projetos de novos diplomas legais capazes de criminalizar tais condutas. Dentre eles o PL 84/1999 e 2.793/2011.

O primeiro trazia a necessidade de elaboração de uma lei específica para penalizar as ações ilícitas realizadas através dos dispositivos eletrônicos. De início, o projeto proposto era muito repressor e pecava pela falta de técnica. Ele também era apontado por suas exigências, consideradas absurdas, as quais tiravam a liberdade dos usuários e provedores de internet, o que o levou a ser apelidado de AI - 5 Digital.

Por conta dessas polêmicas o projeto pouco tramitou até 2011, ano marcado pela ocorrência daqueles que foram considerados os maiores ataques cibernéticos já ocorridos no país.

De junho a agosto de 2011 uma onda de ações promovidas por grupos de *hackers* varreram páginas de órgãos e empresas estatais, fazendo com que estas ficassem temporariamente indisponíveis. O fato serviu de alerta para a situação do Brasil, considerado um país vulnerável a esse tipo de ação, muito em decorrência desse vazio legislativo.

Isso fez reacender as discussões sobre a necessidade de criação de uma legislação voltada para esse universo não tão paralelo. Assim foram retomadas as votações do PL 84/1999 e apresentado o PL alternativo 2.793/2011, o qual era mostrado como o projeto que faria as modificações necessárias, sem que para tanto exigisse os absurdos do anterior.

Contudo, a disponibilidade para a aprovação das leis acabou sendo esvaziada com o fim da onda de ataques, de maneira que os projetos foram de certa forma, “guardados”.

Isso mudou quando um fato caracterizado como ilícito cibernético tomou a mídia. o ocorrido em questão foi a invasão e “furto” de fotos íntimas da atriz Carolina Dieckmann. o que chamou a atenção na época para o fato de não existirem tipos normativos que punissem a invasão e o furto de dados de dispositivo alheio.

A pressão popular causada pela exposição midiática fez com que os projetos fossem votados e aprovados, tornado-se as leis 12.735 e 12.737/2012. A análise dos respectivos diplomas revelou que ainda havia a confusão entre objeto material da norma e bem juridicamente protegido.

Demonstrou, ainda, o desejo de maior agilidade e capacidade de resolução de casos, com a criação de setores da polícia judiciária especializada. Evidenciou ainda, o interesse em evitar que o desenvolvimento tecnológico se prestasse ao aprimoramento dos delitos já combatidos, como o racismo.

Mas o principal avanço do legislador deu-se com a criação dos tipos informáticos próprios, com a tipificação do delito de invasão de dispositivo informático. Como também, a equiparação do cartão de crédito ou débito ao documento particular.

Por fim, em decorrência desse endurecimento legal, espera-se que o usuário ou dependente deste sistema informático, venha a ter mais tranqüilidade ao realizar suas ações. Sem que para tanto, precise preocupar-se com a segurança dos seus dados, sua liberdade de agir, intimidade e privacidade.

7. REFERÊNCIAS BIBLIOGRÁFICAS

ARAS, Vladmir. **Crimes de Informática: uma nova criminalidade**. Revista Eletrônica Jus Navigandi. Publicado em 01 out 2001. Disponível em: <http://juscom.br/revista/texto/225/crimes-de-informatica/5>. Acesso em: 03 dez 2012.

ASIMOV, Isaac. **Eu, robô**. Traduzido por: Jorge Luiz Calif. Rio de Janeiro: Ediouro, 2004.

_____. **O Homem Bicentenário**. Coleção L&PM Pocket, v. 57. Traduzido por: Milton Persson. Porto Alegre: L&PM, 1997.

Bancos perdem R$ 3,1 bi com fraudes eletrônicas. Exame. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/bancos-perdem-r-3-1-bi-com-fraudes-eletronicas>. Acesso em: 10 mar 2013

BRASIL. **Deputado Azeredo**. Câmara dos Deputados. Disponível em: <http://www.camara.leg.br/internet/deputado/Dep.Detalhe.asp?id=530080>. Acesso em: 03 mar 2013.

BRASIL. **Emendas Senado 2793/2011**. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=103616&filename=EMS+2793/2011+%3D%3E+PL+2793/2011>. Acesso em: 08 de mar 2013.

BRASIL**. PL 2557/2000**. Disponível em: <http://www.camara.gov.br/proposicaoWeb/fichadetramitacao?idProposicao=18306>. Acesso em: 06 mar 2013.

BRASIL. **PL 2558/2000**. Disponível em: <http://www.camara.gov.br/proposicaoWeb/fichadetramitacao?idProposicao=18308>. Acesso em: 06 mar 2013.

BRASIL. **PL 2793/2011**. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=529011>. Acesso em: 08 mar 2013.

BRASIL. **PL 3796/2000**. Disponível em: <http://www.camara.gov.br/proposicaoWeb/fichadetramitacao?idProposicao=20236>. Acesso em: 06 mar 2013.

BRASIL. **PLS 76/2000**. Disponível em: <http://www.senado.gov.br/atividade/materia/Consulta.asp?Tipo_Cons=6&orderby=0&Flag=1&RAD_TIP=OUTROS&str_tipo=PLS&txt_num=76&txt_ano=2000.> Acesso em: 08 mar 2013.

BRASIL. **PLS 89/2003**. Disponível em: <http://www.senado.gov.br/atividade/materia/Consulta.asp?Tipo_Cons=6&orderby=0&Flag=1&RAD_TIP=OUTROS&str_tipo=PLC&txt_num=89&txt_ano=2003.> Acesso em: 08 mar 2013

BRASIL. **PLS 137/2000**. Disponível em: <http://www.senado.gov.br/atividade/materia/Consulta.asp?Tipo_Cons=6&orderby=0&Flag=1&RAD_TIP=OUTROS&str_tipo=PLS&txt_num=137&txt_ano=200> Acesso em: 08 mar 2013.

BRASIL. **Projeto de Lei 2793**. Disponível em: <http://www.camara.gov.br/proposicoesWeb/pop_mostraintegra?codteor=944218&filename=Tramitacao-PL2793/2011>. Acesso em: 08 mar 2013.

BRASIL. **Redação Final PL 2793-A**. Disponível em: < http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=992694&filename=TramitacaoPL+2793/2011>. Acesso em: 08 mar 2013.

Brasil está no TOP 5 das corporações vítimas de fraude digital. Convergência Digital. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=33194&sid=18>. Acesso em: 10 mar 2013.

Brasil lidera ataques cibernéticos na América Latina. Disponível em: <http://imasters.com.br/noticia/brasil-lidera-ataques-ciberneticos-na-america-latina/>. Acesso em: 10 mar 2013.

CABETTE, Eduardo L. S. **O novo crime de Invasão de Dispositivo Informático**. Consultor Jurídico. Artigo publicado em 4 de fev 2013. Disponível em: <http://www.conjur.com.br/2013-fev-04/eduardo-cabette-crime-invasao-dispositivo-informatico>. Acesso em: 25 de mar 2013.

CABRAL, Rafael. **Três projetos e duas leis**. Estadão. Disponível em: <http://blogs.estadao.com.br/link/tres-projetos-para-duas-leis/>. Acesso em: 20 mar 2013.

Circuito Digital. Wikipédia. Disponível em: <http:// pt.m.wikipedia.org/wiki/Sistema_digital>. Acesso em: 24 mar 2013.

COLLI, Maciel. Cibercrimes**: limites e perspectivas à investigação policial de crimes cibernéticos**. Curitiba: Juruá, 2010.

DIAS, Tatiana M. **Lei de crimes eletrônicos em regime de urgência**. Estadão. Disponível em: <http://blogs.estadao.com.br/link/lei-de-crimes-eletronicos-em-regime-de-urgencia/>. Acesso em: 20 mar 2013.

Eletrônica. Wikipédia. Disponível em: <http://pt.m.wikipedia.org/wiki/Eletr%C3%B4nica> Acesso em: 24 de mar 2013.

FERREIRA, Aurélio Buarque de Holanda. **Novo Dicionário Eletrônico Aurélio 5.0**. Curitiba: Positivo, 2004. 1 CD-ROM

Fornecedor de acesso à Internet. Disponível em: <http://pt.wikipedia.org/wiki/Fornecedor_de_acesso_%C3%A0_Internet>. Acesso: 06 mar 2013.

GRECO, Rogério. **Curso de Direito Penal: parte especial, volume II: introdução à teoria geral da parte especial: crimes contra a pessoa**. 7ed. Niterói, RJ: Impetus, 2010, p. 64 Apud TOLEDO, Francisco de A. Princípios básicos do direito penal e causas de sua exclusão. Rio de Janeiro: Forense, 1984.

Incidentes reportados por dia da semana. CERT.br. Disponível em: <http://www.cert.br/stats/incidentes/2012-jan-dec/weekdays-incidentes.html>. Acesso em: 10 mar 2013.

Incidentes reportados tipos de ataque. CERT.br. Disponível em: <http://www.cert.br/stats/incidentes/2012-jan-dec/fraude.html>. Acesso em: 10 mar 2013.

Incidentes reportados totais mensais. CERT.br. Disponível em: http://www.cert.br/stats/incidentes/2012-jan-dec/ataques-mensal.html>. Acesso em: 10 mar 2013.

Incidentes Reportados (Top 10 CCs origem de ataques). CERT.br. Disponível em: <http://www.cert.br/stats/incidentes/2012-jan-dec/top-atacantescc.html>. Acesso em: 10 mar 2013.

LEMOS, Rafael. **Roubo de fotos de Carolina Dieckmann acelera tramitação de projeto de lei sobre crimes cibernéticos**. Veja. Disponível em: <http://veja.abril.com.br/noticia/brasil/roubo-de-fotos-de-carolina-dieckmann-acelera-tramitacao-de-projeto-de-lei-sobre-crimes-ciberneticos>. Acesso em: 20 mar 2013.

LIMA, Paulo M. F. **Crimes de Computador e Segurança Computacional**. Campinas: Millennium Editora, 2005.

LOPES JUNIOR, Aury. **Direito Processual Penal e sua conformidade constitucional**. V. 1. 5.ed. ver. e atual. Rio de Janeiro: Lumem Juris, 2010.

Maior ataque hacker no Brasil partiu da Itália. Revista Época. Disponível em: <http://revistaepoca.globo.com/Revista/Epoca/0,,EMI243559-15224,00.html>. Acesso em: 10 mar 2013.

MARQUES, Jéferson. **Operação #AntiSec começo, meio e o fim?** Disponível em: <http://www.plantaonerd.com/blog/2011/06/24/artigo-operacao-antisec-comeco-meio-e-o-fim-moderar/>. Acesso em: 10 mar 2013.

MATRIX. Direção de Andy, Lana Wachowski. Produção de Bruce Berman. USA, Austrália: Warner Bros. Pictures, Village Roadshow Pictures, 1999. 1 videocasset.

MENEZES, Tyndaro; Soares, Paulo R. **Polícia encontra hackers que roubaram fotos de Carolina Dieckmann**. Fantástico. Disponível em: <http://g1.globo.com/fantastico/noticia/2012/05/policia-encontra-hackers-que-roubaram-fotos-de-carolina-dieckmann.html>. Acesso em: 20 mar 2013.

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

MIRANDA, Murilo. **Da persecução penal dos crimes virtuais**. Jus Way: sistema educacional online. Publicado em 27 de janeiro de 2013. Disponível em: < http://www.jurisway.org.br/v2/dhall.asp?
id_dh=9903>. Acesso em: 17 de abr 2013.

O que é um servidor de internet? Palpite Digital.Com. Disponível em: <http://www.palpitedigital.com/o-que-e-um-servidor-de-internet/>. Acesso em: 06 mar 2013.

Peer-to-Peer. Disponível em: <http://pt.wikipedia.org/wiki/Peer-to-peer>. Acesso em: 07 mar 2013.

Projeto Azeredo: Ato Contra o AI-5 Digital dia 14, em São Paulo, 3 junho de 2009. Software Livre Brasil. Disponível em: <http://softwarelivre.org/portal/legislativo/projeto-azeredo-ato-contra-o-ai-5-digital-dia-14-em-sao-paulo.> Acesso em: 06 mar 2013.

Senado aprova Lei Carolina Dieckmann sobre crimes de internet. Bom Dia Brasil. Disponível em: <http://g1.globo.com/bom-dia-brasil/noticia/2012/11/senado-aprova-lei-carolina-dieckmann-sobre-crimes-de-internet.html>. Acesso em: 08 mar 2013

Senador Magno Malta denuncia à PF invasão de hackers a seu site. Portal G1. Disponível em: <http://g1.globo.com/tecnologia/noticia/2011/06/senador-diz-que-denunciou-pf-invasao-de-hackers-seu-site.html>. Acesso em: 21 mar 2013

Site do IBGE permanece fora do ar após ataque de hackers. Veja. Disponível em: <http://veja.abril.com.br/noticia/brasil/site-do-ibge-permanece>. Acesso em: 10 mar 2013.

Tentativas de fraudes reportadas. CERT.br. Disponível em: <http://www.cert.br/starts/incidentes/2012-jan-dec/fraude.html>. Acesso em: 10 mar 2013.

Valores acumulados: 1999 a dezembro de 2012 novo. CERT.br.Disponível em: <http://www.cert.br/stats/incidentes/#2012>. Acesso em: 10 mar 2013.

WENDT, Emerson e JORGE, Higor V. N. **Crimes Cibernéticos: ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport, 2012.

ZANIOLO, Pedro A. **Crimes Modernos: o impacto da tecnologia no Direito**. Curitiba: Juruá, 2007.

@LulzSecBrazil. Disponível em: <http://www.twitter.com/LuIzSecBrazil>. Acesso em: 10 mar 2013.