CRIMES CIBERNÉTICOS

HARACEMIW, Rafael Antônio[1]
VIEIRA, Tiago Vidal[2]

RESUMO

O presente trabalho faz uma análise de como surgiram, assim como a forma com que eram tratados os crimes virtuais antes da promulgação da Lei 12.737/2012, e como passaram a ser analisados e julgados com o advento dela. O objetivo é analisar o que mudou com a Lei dos crimes virtuais, apelidada de "Carolina Dieckmann". Os crimes cibernéticos são aqueles cometidos através de dispositivos eletrônicos, e contra eles, sendo por exemplo, computares, *tablets*, celulares, entre outros. Inicialmente, é tratado sobre a evolução histórica da tecnologia e como ela acarretou no desenvolvimento da internet e por consequência como isso afetou a legislação vigente. Por fim é feita uma análise comparando as diferenças de como o Brasil e outros países lidam com os delitos informáticos, bem como a referida Lei é avaliada, tratando sobre as críticas por ela sofridas, bem como, os benefícios por ela trazidos. A técnica empregada para a elaboração do estudo é a bibliográfica, com fontes em livros, leis, decretos, artigos científicos e artigos em *internet*.

PALAVRAS-CHAVE: Crime Cibernético; tecnologia; Lei nº 12.737/12.

CYBER CRIMES

ABSTRACT

The research deals with crimes committed through electronic devices, and against them, for example, computers, tablets, phones, among others, doing analysis of how they came about, as well as how they were treated before the enactment of Law 12,737 / 2012, and how passed to be analyzed and judged with the advent of her. The objective is to analyze what has changed with the Law of cybercrime, dubbed "Carolina Dieckmann". Initially, deals about the historical evolution of technology and how it resulted in the development of the internet and therefore how it affected current legislation. Finally an analysis will be done comparing the differences of how Brazil and other countries deal with computer-related crimes, as well as how is evaluated the Law of cyber crimes, treating about criticism suffered by it as well, the benefits brought by it. The technique employed for the preparation of this work is the bibliographic, with sources in books, laws, decrees, scientific papers and articles in internet.

KEYWORDS: Cyber crimes; Tecnology; Law 12.737/12.

1 INTRODUÇÃO

A internet é sem dúvida a grande invenção do homem no século XX, com ela houve um enorme salto tecnológico em tudo o que rege a sociedade e, como toda grande invenção, junto aos prós vieram os contras, e como não poderia ser diferente a internet trouxe grande repercussão ao Direito Penal e Processual Penal, pois com ela várias formas de delitos se tornaram muito mais comuns e recorrentes no cotidiano da população em escala mundial, mas talvez no Brasil tenha se dado de forma um pouco mais abrangente, em consequência da grande impunidade, corrupção e falta de investimentos por parte do governo nas áreas de segurança e tecnologia, que acarretaram em um grande atraso jurídico no tocante a regulamentação desses delitos cometidos através dos meios informáticos e que mesmo após regulamentados continuam gerando impunidades, vez que as leis não foram escritas de forma clara e abrangente, além de haver nenhum esforço que mereça respeito por parte do governo no tocante a criar mecanismos e sistemas de capacitação dos agente públicas afim de que se tornasse plenamente possível a investigação e a prevenção adequadas destes delitos.

O assunto está relacionado ao Direito Penal, ramo do Direito ao qual se incumbe à tarefa de cuidar dos crimes, sendo desta forma, a área responsável por garantir que os crimes virtuais não fiquem impunes por falta de legislação específica.

Em suma os crimes virtuais são aqueles que atingem de forma direta ou indireta, a intimidade, a honra, o patrimônio e os dados pessoais da vítima, sendo cometidos através da internet ou de equipamentos eletronicos. Por serem crimes de contextualidade nova ainda é pouco estudado, entretanto, se mostram de vital importância no cotidiano do homem moderno.

O potencial de causar danos desta modalidade criminosa tem se mostrado muito elevado, ao fato de que atualmente todas as empresas e pessoas físicas utilizam dispositivos eletrônicos para armazenar seus dados, por conta disso, a comunidade jurídica e a própria sociedade em geral, vinham aclamando cada vez mais pela criação de uma Lei regulamentadora das ações delituosas cometidas através de dispositivos eletrônicos em virtude do grande e crescente número de crimes cometidos no *cyber* espaço.

Os crimes cometidos através de dispositivos eletrônicos sejam eles, computadores, *tablets*, celulares, e qualquer outro dispositivo capaz de armazenar dados, ou fazer comunicação com outro semelhante, é tema desta análise da Lei

[1] Acadêmico – Faculdade Assis Gurgacz rafaelharacemiw@gmail.com
[2] Docente orientador – Faculdade Assis Gurgacz Curso de Direito

dos Crimes Cibernéticos (Lei n°12.737/2012), expondo os benefícios por ela trazidos, assim como as críticas quanto a sua redação.

O presente trabalho visa expor o grave problema que esses crimes se tornaram e a grande dificuldade em que a polícia tem em combatê-los, devido ao pouco caso em que o governo apresenta diante desta situação e a sua falta de investimentos em treinamento de pessoas qualificadas e equipamentos específicos para este fim, bem como faz uma breve comparação de tempo e de como o tema é tratado no Brasil e em outros países.

2 DESENVOLVIMENTO

2.1. EVOLUÇÃO HISTÓRICA DA *INTERNET*

Impossível não admitir que a *internet* foi a melhor evolução que aconteceu no último século, o homem atual dificilmente se adaptaria novamente a um mundo sem ela, seus benefícios foram incalculáveis, aproximou o mundo todo, acelerou as pesquisas tecnológicas, facilitou contatos, entre outros benefícios.

Por volta dos anos 50, durante o período de Guerra Fria entre os EUA e URSS, aconteceu uma grande corrida armamentista e tecnológica causada pelo iminente risco de uma guerra. Durante este período de tensão, a necessidade de comunicação entre as pessoas sempre foi algo de vital importância e sua evolução sempre foi muito almejada, como a comunicação fácil e rápida se tornou algo muito necessário, a *internet* foi criada pelos americanos como uma forma de resposta ao lançamento do satélite *Sputinik* pela ex – União Soviética.

A princípio a ideia era conectar os mais importantes centros universitários de pesquisa americanos com o Pentágono, para permitir além de uma comunicação rápida e segura, uma instrumentalização do país com uma tecnologia que permitisse a sobrevivência de canais de comunicação em caso de haver uma guerra nuclear.

Os criadores do projeto jamais poderiam imaginar que tal dispositivo tomaria à proporção que a *internet* possui hoje devido à complicada linguagem usada nos computadores ligados à rede. Durante os anos 1970 e 1980 tal linguagem se tornou mais simples, sendo criados programas, e o sistema de e-mail que se tornou muito comum entre os pesquisadores da época, pois permitia uma fácil comunicação entre eles, além da troca de informações de forma segura e precisa dentro das universidades.

Durante os anos 1980 começaram a surgir os primeiros provedores de *internet* que permitia a qualquer usuário acesso à rede mundial de computadores de dentro de suas casas.

Em meados de 1992 o W W W (*World Wide Web*) foi lançado e gerou um notório aumento de servidores, depois disso a internet não parou mais de crescer, se expandindo para o mundo inteiro e se tornando fundamental no cotidiano de praticamente toda a sociedade.

Com efeito, o espantoso e contínuo desenvolvimento da informática e da telecomunicação, decorrentes de uma verdadeira revolução tecnológica, proporcionou a utilização cada vez maior, mais disseminada e liberalizada do computador, com isso unido as tecnologias de comunicação, é ofertado a todos um potencial de acesso imediato e, praticamente ilimitado às informações.

Tal comodidade trouxe várias mudanças ao cotidiano do homem hodierno, conforme assinala Luis Regis Prado (2013):

> A evolução constante do sistema informático pode apresentar diferentes consequências no mundo jurídico em geral, A primeira, de feição positiva, diz respeito à informatização e armazenamento de dados, a praticidade e celeridade no acesso à informações processuais e o próprio processo eletrônico. A segunda, consequência, de cunho negativo, é traduzida na facilitação dos meios para se praticar delitos. Isso se dá em diversas áreas de criminalidade, como, por exemplo, criminalidade patrimonial e econômica – em que os procedimentos informáticos são utilizados para realização de operações comerciais irregulares e prejudiciais, para a pirataria, transações em bolsas de valores, etc.; criminalidade não patrimonial, onde se pode visualizar finalidades lucrativas, como tráfico de drogas, tráfico de pessoas, pornografia infantil, violação de direitos de imaginem, falsidades, crimes contra a honra.

2.2. EXPLANAÇÃO ACERCA DOS CRIMES CIBERNÉTICOS

No âmbito jurídico a evolução da *internet* não poderia ser diferente e a adesão aos equipamentos eletrônicos tornou os processos mais céleres e seguros em todos os ramos do Direito, a exemplo disto temos de maneira ampla toda a sistematização da maioria dos processos, ou em aspectos mais restritos, a exemplo do Direito Civil, em relação ao comércio eletrônico e por consequência às relações consumeristas, grande alvo de estelionatários, que através deste

meio criam e espalham pela rede várias páginas com conteúdo falso e empresas de fachada, que visam ludibriar e roubar quem usa este meio, envolvendo então, as áreas do Direto Penal e Processual Penal.

Para o Direito Penal e Processual Penal toda a evolução tecnológica que foi ocasionada pela internet se deu principalmente de uma forma negativa, pois os crimes que antes dela já eram difíceis de combater, como é o caso do estelionato, que geralmente é cometido contra vítimas com pouco conhecimento e que se sentem extremamente envergonhadas em admitir que foram lesadas por esta forma de golpe, piorou muito com o surgimento da *internet* e dos novos dispositivos eletrônicos, pois se tornaram ainda mais difíceis de serem suprimidos, em vista de que, os autores dos delitos normalmente utilizam nomes falsos, e através de paginas da *internet* ou até mesmo pelo telefone contatam as pessoas e induzindo-as ao erro as roubam.

É indiscutível que os *cyber* crimes tornaram-se um dos mais graves problemas sociais da atualidade e com grande potencial de evoluir e se tornarem cada vez mais perigosos, diante de toda a evolução tecnológica que o mundo ainda vem sofrendo, tornando o índice de impunidade ainda mais elevado já que poucas vitimas denunciam os crimes eletrônicos.

Toda essa tecnologia acabou por criar um novo instrumento para as ações delituosas de crimes já previstos pelo Código Penal, a exemplo disso temos os crimes mais comuns cometidos através dos dispositivos informáticos, que são a fraude, os crimes cometidos contra a honra e o furto, que podem ser cometidos sem que a vítima veja sequer o rosto do criminoso, e para tornar ainda mais crítica a situação a polícia judiciária não possui os mecanismos necessários para buscar através de peritos os autores dos crimes.

Salienta-se ainda que o Direito Penal em respeito ao princípio da legalidade e visando buscar a verdade real dos fatos, para então julgar de forma justa, não avalia condutas através de analogia *in malam partem*, tal como, claramente expressa a Carta Magna, em seu artigo 5°, XXXIX “Não haverá crime sem lei anterior que o defina, nem pena sem prévia cominação legal”, desta forma, cria-se uma enorme brecha no ordenamento jurídico gerando grande probabilidade desses crimes ficarem impunes e com isso, estabelece-se de certa forma uma comodidade aos criminosos para cometer esses crimes.

Contudo, na prática, a Polícia para evitar que os crimes cometidos por meio de dispositivos informáticos ou que fossem cometidos contra eles, não ficassem impunes antes da Lei 12.737/12 ser sancionada, enquadrava os autores, quando encontrados, em outros tipos penais, por exemplo, quando alguém tinha seu patrimônio lesado através de um golpe na *internet*, os autores eram processados pela prática do crime de estelionato, ou seja, os crimes cometidos por meios eletrônicos que ainda não contavam com uma legislação específica, eram enquadrados em outros tipos penais já existentes, sendo assim, aquele que lesava alguém se valendo de um dispositivo informático, seja invadindo-o ou se utilizando dele para instalar vulnerabilidades em dispositivo alheio visando a obtenção de vantagem ilícita era processado e julgado através de crimes já previstos no CP.

2.3. A CRIAÇÃO DA LEI

A referida Lei foi criada em 2011 através do projeto Nº. 2793, tendo como autor o deputado federal Paulo Teixeira, sendo aprovada em 2012 sem vetos, com o período de vacância de 120 dias, o projeto deu origem à lei 12.737 aprovada em 30 de Novembro de 2012, que veio para tipificar os delitos informáticos, alterando o Decreto-Lei Código Penal N°. 2.848, de 7 de Dezembro de 1940, dando novas providências a estes crimes.

À medida que recebeu o nome da atriz Carolina Dieckmann, em virtude da grande repercussão midiática criada em torno de seu caso, o que acabou dando ao projeto maior velocidade à tramitação do processo legislativo, que foi votado e sancionado durante as investigações e julgamento do caso em que atriz teve seu computador violado, e, suas fotos íntimas roubadas e amplamente expostas na *internet* por um criminoso que a chantageou pedindo dinheiro como troca para que as fotos não fossem publicadas na rede.

A nova Lei acrescentou ao Código Penal, dois novos artigos: 154-A e 154-B, que apesar de estarem presentes no Titulo I, da parte especial do CP, que se refere aos crimes contra honra, não se enquadram perfeitamente ao titulo, pois além de protegerem a intimidade, a vida privada e o direito ao sigilo de dados constantes em dispositivos informáticos, tutelam também o patrimônio do titular do dispositivo violado, na medida em que pune o intuito do agente de obter vantagem ilícita.

Os delitos informáticos possuem fácil identificação em virtude da forma e do meio empregado para cometê-los, bem como frente ao seu grande potencial danoso, por exemplo, se um *cracker*[3] se valendo apenas de seus conhecimentos informáticos invade o sistema de uma empresa de telefonia, que tem seu sinal ligado diretamente às

[3] Os crackers são pessoas aficionadas por informática que utilizam seu grande conhecimento na área para quebrar códigos de segurança, senhas de acesso a redes e códigos de programas com fins criminosos.

redes de *internet*, causará prejuízos de grande monta não só para a empresa como também para um enorme numero de pessoas que utilizam os serviços desta empresa.

Contudo, da mesma forma que é fácil identificar um crime cibernético, a identificação do autor do delito é praticamente impossível, tendo em vista que para acessar a *internet* não há nenhuma forma de controle e nem a necessidade de identificação. Desta forma qualquer pessoa pode ser autora do crime, e sua identificação é muito difícil, pois os usuários se conectam a rede através de uma tecnologia conhecida como *Tcp/ip* (*transmission control protocol – internet protocol*) cujo software normalmente reside no sistema operacional, onde todos os programas e aplicativos utilizados na máquina compartilham do mesmo número (*ip*) que é único e se altera automaticamente a cada novo acesso a *internet*, sendo assim o agente pode se conectar de qualquer dispositivo eletrônico e de qualquer lugar cometer o ilícito penal utilizando apenas conhecimentos próprios e se valendo indiscriminadamente desse meio ciente de que após cometer a infração e se desconectar da *internet* a única forma possível para sua identificação, ou seja, o número de *ip* utilizado momentos antes pelos programas empregados na prática delituosa foi apagado, sendo gerado um novo *ip* em uma conexão a *internet* futura.

2.4. AS ESPECIFICIDADES DA LEI

No crime em questão, adicionado ao Código Penal pela Lei 12.737/12, considera-se que pode incorrer como sujeito ativo qualquer pessoa, já que o seu tipo penal não exige nenhuma qualidade especial do seu agente, sendo portanto um crime comum.

Quanto ao sujeito passivo dos crimes informáticos considera-se que possa ser qualquer pessoa que utilize ou não o meio eletrônico, podendo existir mais de um indivíduo desde que tenham seus bens jurídicos ameaçados ou lesados pela mesma conduta delituosa, como por exemplo, uma série de *e-mails* contendo o mesmo conteúdo viral cujo objetivo é lesar quem os recebe.

O bem jurídico tutelado pela Lei em questão, como bem explica Eduardo Luiz Santos Cabette:

> é a liberdade individual, eis que o tipo penal está exatamente inserido no capítulo que regula os crimes contra a liberdade individual (artigos 146 – 154, CP), em sua Seção IV – Dos Crimes contra a inviolabilidade dos Segredos (artigos 153 a 154 – B, CP). Pode-se afirmar também que é tutelada a privacidade das pessoas (intimidade e vida privada), bem jurídico albergado pela Constituição Federal em seu artigo 5º, X., havendo portanto uma tutela individual dos interesses das pessoas físicas e/ou jurídicas, nada tendo a ver com a proteção à rede mundial de computadores e seu regular funcionamento.

Os crimes criados através da Lei 12.737/12 são crimes formais em sua forma simples, pois não exigem no tipo básico resultado naturalístico para a consumação e, portanto, se consumam com a mera invasão ou instalação de vulnerabilidade no equipamento eletrônico, não sendo necessário alcançar o objetivo do feito, sendo que tais resultados constituem mero exaurimento da infração em estudo. Já a forma qualificada dos delitos se trata de crimes materiais, por exigirem para a consumação a obtenção efetiva de conteúdos ou o controle não autorizado do dispositivo invadido.

O ilícito também admite a forma tentada, pois é plenamente possível que pessoa tente invadir um sistema ou instalar vulnerabilidades e não consiga por motivos alheios a sua vontade, seja por ser fisicamente impedida ou por não conseguir violar os mecanismos de proteção criados para evitar as invasões.

O tipo subjetivo do ilícito ocorre apenas na forma dolosa, não havendo a possibilidade de ocorrer na modalidade culposa, pois a lei exige que a violação se dê com o especial fim de "obter, adulterar ou destruir dados ou informações" ou "instalar vulnerabilidades para obter vantagem ilícita", havendo, portanto, nas duas formas, requisitos que o agente deve cumprir para que haja o delito.

Tal legislação, primeira no combate de crimes na *internet*, estabelece para a parte do caput do artigo 154-A, do CP, o qual define como crime a ação de invadir dispositivo informático, conectado ou não à *internet*, mediante violação de mecanismos de segurança, ou instalar neles vulnerabilidades, com o fim de obter vantagens ilícitas, assim como, para seu parágrafo 1º pena de detenção de 03 (três) meses a 1 (um) ano, e multa, sendo aumentada de 1/6 a 1/3 caso a invasão resulte em prejuízo econômico, sendo desnecessário que haja efetivamente obtenção, adulteração, destruição de dados ou informações, ou obtenção de vantagem ilícita (delito de mera atividade). Incorre ainda na mesma pena quem produzir, oferecer, distribuir, vender ou difundir dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput, conforme expresso o parágrafo 1º. A tentativa é admissível, e se verifica quando a invasão ou instalação não ocorre por circunstâncias alheias à vontade do agente.

O dispositivo de Lei ainda oferece a forma qualificada do crime, constantes nos parágrafos 3° e 4° do dispositivo Penal supracitado, dos quais se extrai que "se da invasão resultar na obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto de dispositivo não autorizado", a pena de reclusão será de 6 (seis) meses a 2 (dois) anos, e multa, sendo aumentada de 1 a 2

terços se houver divulgação, comercialização, ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas, caso a conduta não constitua crime mais grave.

Por fim o §5° do referido artigo aumenta a pena de um terço a metade se o crime for praticado contra os presidentes do poder legislativo e judiciário, assim como os dirigentes máximos da administração direta e indireta, englobando-os na tanto na esfera federal, quanto na estadual, municipal ou do Distrito Federal.

Para haver a ação penal, a vítima deverá necessariamente representar, ou seja, deverá obrigatoriamente prestar queixa crime em uma delegacia para que ocorra a investigação e posteriormente o julgamento do crime, salvo nos casos em que o crime for cometido contra a administração pública direta ou indireta de qualquer dos poderes da União, Estados, Distrito Federal ou Municípios, ou ainda contra empresas concessionárias de serviços públicos, casos estes em que não é necessária a representação.

A nova Lei ainda alterou a redação do artigo 266 do Código Penal, que acrescentou ao crime de "interrupção ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento", o parágrafo 1° que dispõe que incorrerá na mesma pena aquele que interrompe serviço telemático ou de informação de utilidade pública, ou impedir ou dificultar-lhe o restabelecimento, bem como também acrescentou ao artigo 298 o parágrafo único, o qual dispõe que para fins de falsificação ou alteração, equiparasse o documento particular o cartão de crédito ou débito.

Ante o exposto, explana Luiz Regis Prado (2013) que:

> Torna-se necessária, inadiável mesmo, a intervenção do Direito Penal – técnica e cautelosa – para prevenir e sancionar condutas que atentam gravemente contra bens jurídicos relevantes.

2.5. DO CRIME

O crime consiste em invadir dispositivo informático alheio, estando ou não conectado à *internet*, por meio de violação indevida de mecanismo de segurança estabelecido pelo proprietário do dispositivo, salienta-se ainda que para ocorrer o delito, o agente deve objetivar a obtenção, adulteração ou destruição dos dados ou informações, ou ainda instalar vulnerabilidades para obter vantagens ilícitas, sendo estes, a inserção de programas executáveis, que visam a captação de senhas e dados alheios, havendo portanto duas descrições típicas distintas no mesmo tipo penal, sendo que a primeira (invadir dispositivo alheio) se consuma no momento da efetiva invasão, não sendo necessária a obtenção da vantagem ilícita pretendida e no segundo (instalar vulnerabilidades) irá se consumar no momento da instalação da vulnerabilidade, também não sendo exigível a ocorrência do resultado naturalístico pretendido pelo agente, sendo portanto, ambas descrições consideradas formais.

Conforme preceitua Fernando Capez (2013):

> O núcleo central da conduta típica consubstancia-se no verbo "invadir", isto é, ingressar virtualmente, sem autorização expressa ou tácita do titular do dispositivo".
> "A conduta de invadir traz ínsita a ausência de autorização do proprietário ou usuário do dispositivo, pois não se pode dizer que houve invasão quando o acesso se dá mediante sua aquiescência. Mesmo assim, o tipo penal do art. 154-A, caput, do CP, de modo supérfluo, repete ao final a exigência do elemento normativo do tipo "sem autorização expressa ou tácita do titular do dispositivo.

2.6. COMO OS CRIMES CIBERNÉTICOS ERAM TIPIFICADOS ANTES DA CRIAÇÃO DA LEI

Antes da Lei 12.737/12 (Lei dos Crimes Cibernéticos) ser sancionada, vários crimes que já eram tipificados no Código Penal adquiriram uma nova roupagem com o advento da *internet* e com o uso de meios informáticos, tornando muito mais difícil para a policia a investigação e o descobrimento dos autores dos delitos, além de que, quando descobertos, tinham um julgamento muito truncado cheio de barreiras e empecilhos, pois por não possuírem tipos penais próprios encontravam diversos obstáculos durante o processo penal, já que eram julgados através de analogia, onde os crimes de subtração de dados de um computador eram equiparados ao crime de furto e a inutilização de dados do computador ao crime de dano, contudo, ambas as formas não obteveram muito sucesso perante os tribunais já que em virtude da atipicidade dos crimes esbarravam no artigo 5º, inciso XXXIX, da Constituição Federal.

Segundo Mirabetti, para configurar o crime de dano é necessário que haja pelo menos uma das três condutas descritas no tipo penal, quais sejam: destruir, inutilizar ou deteriorar, o que não ocorre nos delitos de invasão de equipamentos eletrônicos com o intuito de roubar arquivos digitais, já que o furto dos arquivos não significa que haverá a sua deterioração ou inutilização, o que deixava claro a necessidade de tipificar o ato afim de proteger o usuário frente a impossibilidade do enquadramento da conduta de crime informático no crime de dano.

Insta salientar que em alguns casos foi possível enquadrar o agente que utilizava acesso indevido, para invadir computadores de instituições bancárias e desviar dinheiro para outras contas, por furto, mas o enquadramento no tipo penal de furto só era possível pelo furto do dinheiro e não pelo "furto" de dados do computador que era uma conduta atípica, sendo assim, se houvesse apenas o roubo de dados, de empresas ou simplesmente dados pessoais de pessoas, não haveria crime face a falta de codificação legal.

2.7. DIREITO COMPARADO – COMO FUNCIONA A LEGISLAÇÃO DE CRIMES INFORMÁTICOS EM OUTROS PAÍSES

Um dos grandes motivos da Lei dos Crimes Cibernéticos sofrer tantas críticas são as lacunas deixadas por ela em temas de vital importância para o atual momento em que vive o direito brasileiro, sendo que a principal razão para a existência dessas lacunas, segundo os autores especializados sobre o tema é a grande velocidade com que a Lei foi elaborada aliada ao descaso dos legisladores responsáveis pela criação desta, fatos que não deveriam ter ocorrido, face ao longo tempo que tiveram para a sua criação já que sua publicação se comparada a tantos outros países que lidam a muito mais tempo e de forma muito mais eficiente com esse problema se deu de uma forma muito tardia, além da enorme necessidade de se ter uma Lei competente postulando sobre esses delitos no direito brasileiro já que se trata de um tema tão recorrente, antigo e já comum para toda a população. Cabe ainda acrescentar que há muito tempo o sistema legislativo brasileiro poderia ter usado um direito estrangeiro como base e regulamentado toda essa situação de forma muito eficiente.

Como primeira comparação temos os EUA com o seu bem sucedido direito baseado no Common Law – modelo de justiça baseado em precedentes judiciais, o qual é bastante complexo pois há tribunais com maiores poderes que outros, como é o caso dos tribunais recursais, tal como, há ainda como normas penais, as leis já codificadas e os ilícitos que decorrem de decisões judiciais. Como bem se sabe os Estados Unidos utiliza a politica do federalismo, na qual é permitidos que todos os estados criem suas próprias regras sem que seja preciso utilizar o processo legislativo, ou seja, cada estado é capaz de criar suas próprias leis, neste modelo de direito é possível a criação de leis e direitos a partir de uma decisão judicial que sirva como precedente.

O EUA é considerado o pioneiro no combate a crimes cibernéticos, e acredita-se que com eles aconteceram as primeiras manifestações informáticas ilegais, surgindo no final dos anos 70 com um estudante chamado Robert Tappan Morris, que começou a trabalhar em programa de computador, explorando as falhas de segurança que havia descoberto na *internet*, com o intuito de demonstrar como eram inadequadas as medidas de segurança empregadas na rede. Seu programa criou os "*worms*" que era um vírus capaz de se proliferar e se espalhar pelos computadores com o objetivo de apenas ocupar uma parte do funcionamento das maquinas, mas seu experimento tomou proporções maiores e ele perdeu o controle, causando grande prejuízo às redes de computadores da época.

A partir de então o país começou a combater seriamente os crimes informáticos, sendo criados mecanismos federais através da Lei de Proteção aos Sistemas Computacionais (*Federal Computer System Protection*) em 1981, e estaduais em 1982 com a Lei *Eletronic Funds Transfer*, a qual regulamenta as transferências eletrônicas de fundos, incriminando as fraudes informáticas que não continhas relações interpessoais.

Mas a principal Lei estadunidense que trata de crimes informáticos surgiu em 1986, muito antes de se discutir qualquer coisa sobre o tema no Brasil, sendo ela a Lei de Fraude e Abuso Computacional (*Computer Fraud and Act*), que visa proteger a acessibilidade dos sistemas, da obtenção ilícita de segredos nacionais ou da tentativa de obter vantagens financeiras, através do meio eletrônico.

A Suécia através de seu código *Rättgangsbalken* considerado moderno a época de sua entrada em vigor, se antecipou aos delitos informáticos e até mesmo ao desenvolvimento do computador e em 1948 criou uma Lei que embora não trata-se de forma direta sobre os crimes cibernéticos, foi capaz de rege-los logo após o seu surgimento, protegendo de forma eficiente todos os dados armazenados nos dispositivos eletrônicos e lidando de forma precisa com todas as relações que decorreram do surgimento da *internet* e dos equipamentos eletrônicos. Tal Lei foi tão bem elaborada que era ainda capaz de ser aplicada tanto na esfera cível quanto na penal.

Já o Direito Italiano, há cerca de 20 anos sofreu uma grande mudança passando do sistema inquisitorial para o acusatório, eliminando totalmente o autoritarismo que o antigo código continha o que tornou possível que em 1993 fossem criadas Leis mesmo que pouco simples, mas que tratavam de crimes informáticos, contudo, mesmo antes de as Leis serem sancionadas, o Direito italiano reconheceu a necessidade de adaptar os dispositivos que continham em seu bojo a tipificação das fraudes, para assim enquadrar os crimes informáticos de forma extensiva e então poder acompanhar os avanços tecnológicos, o que não foi possível fazer no Brasil, por não encontrar boa vontade por parte dos poderes legislativo e executivo do país.

2.8. CRÍTICAS E SOLUÇÕES ACERCA DA NOVA LEI

Para Afonso Silva, presidente da comissão de Direito Eletrônico,

> a iniciativa para coibir esse tipo de crime é louvável, mas esta lei surgiu de forma muito rápida, sem muitas discussões em torno do tema, o que deixa pontos a serem debatidos, Afirma ainda que de nada adianta a lei se o usuário não se proteger. É preciso adotar práticas de segurança, como a criação de senhas e proteção dos arquivos, pois, de acordo com o a lei, somente será crime se o dispositivo for invadido por meio de quebra de senhas. Ou seja, se o fraudador não enfrentar barreiras para acessar os arquivos, não será considerado crime.

Portanto, o que se aconselha aos usuários é que sempre mantenham um antivírus atualizado, e que elaborem nos arquivos senhas que não contenham informações básicas, como telefone e aniversário, pois é fato que os crimes aqui apresentados só ocorrem com a colaboração do usuário, em seu desleixo ou falta de atenção ao que acessa, ou arquiva em seu computador, *tablet* etc. desta forma, o simples fato de os usuários deixarem de clicar em um link que pareça suspeito, já contribui em muito para a redução desta modalidade delituosa.

Outro grave problema apontado pelo especialista Armando de Vilhena, diretor executivo da empresa de segurança TIX 11, é o fato de que a lei restringe o ato criminoso. Segundo o artigo 1º da nova lei, somente é considerado crime se o dispositivo - conectado ou não a uma rede de computadores - for invadido por meio de quebra de senha ou de outros mecanismos de proteção.

> O problema disso é que, se você deixar o acesso à máquina livre, com o usuário desprotegido, e o fraudador não tiver que romper uma barreira para acessá-la, isso não será considerado crime. É o mesmo que deixar a sua carteira por alguns segundos em cima da mesa e alguém pegá-la", disse Vilhena. "A lei está muito vinculada a uma quebra explícita de mecanismo de segurança e isso pode gerar problemas. Principalmente para usuários domésticos, que costumam não utilizar senhas em seus dispositivos.

Um detalhe importante que deve ser observado, que difere este tipo penal de outros tipos penais comuns, é a elementar “mediante violação indevida de mecanismo de segurança”, isso significa que só haverá o crime do art. 154 do CP se o autor da conduta usar sua habilidade para superar a proteção do sistema informático, por mais simples que ela seja, pois se caso o dispositivo estiver completamente desprotegido, não haverá a invasão e, portanto não haverá crime, uma vez que não foi cometido mediante violação de segurança.

Cabe mencionar ainda o fato de que se o criminoso conseguir fazer com que a vítima lhe entregue as informações que precisa, ou ainda que ela mesma desabilite os sistemas de proteção para que ele possa acessar livremente seu dispositivo, mesmo que não ocorra a invasão do dispositivo eletrônico, o agente responderá pelo crime do artigo 154-A do CP, em vista de que a vítima foi induzida a erro e não agiu de forma consciente, pois neste caso considera-se que ocorreu a violação indevida da segurança do computador, contudo, se o agente com habilidade, conseguir que a vítima lhe envie o conteúdo, sem que haja invasão, não haverá o crime por ausência do verbo núcleo do tipo penal (invadir). Seguindo o mesmo raciocínio, o agente que instalar vulnerabilidades em dispositivo alheio, só incorrerá no crime se trouxer consigo a respectiva finalidade que é a de obter vantagem ilícita, ao passo que se a sua intenção é de apenas deixar o dispositivo vulnerável, não haverá o crime, porém, isso não significa que seja necessária a obtenção de vantagem ilícita ou de informações para a consumação do crime, se tratando, portanto, de um crime formal, ou seja, não sendo necessária a consumação do delito para que ele ocorra, sendo esses resultados considerados meros exaurimentos do crime.

Tentando iniciar a solução para o enorme problema social que se tornaram os crimes cibernéticos juntamente com a Lei “Carolina Dieckmann” foi votada e aprovada a Lei 12.735/12 denominada de Lei “Azeredo”, a qual determinou que os órgãos da polícia judiciária deverão estruturar, nos termos de regulamentos, setores e equipes especializadas no combate à ações delituosas na rede de computadores, dispositivos de comunicação ou sistemas informatizados.

O governo brasileiro agiu de forma omissa perante a grande popularização da *internet* e sua rápida disseminação deixando de investir em mecanismos para controlar o que ocorre na rede, bem como não capacitou a polícia judiciária para lidar com essa nova modalidade criminosa, e não criou delegacias especificas suficientes para investigar e proteger os usuários destes crimes.

3 CONSIDERAÇÕES FINAIS

Ante todo o exposto percebe-se os grandes avanços que *internet* proporcionou, assim como os vários problemas que foram gerados por ela. Sua criação foi de grande importância para o direito brasileiro, com toda a sistematização dos processos e agilidade proporcionada que fez do judiciário um órgão mais célere e portanto mais justo.

Junto com todos os benefícios gerados, a *internet* junto com os novos e modernos equipamentos eletrônicos desencadeou uma série de novos processos gerados por crimes ainda não codificados, os chamados crimes virtuais, que no Brasil levaram um tempo demasiado grande para serem estudados e tipificados, fato este que entre o período do surgimento da *internet* e a criação das Leis responsáveis por regularizar e proteger os bens afetados pelos crimes virtuais gerou uma grande onda de impunidade e descontrole por parte dos usuários mal intencionados. O judiciário por mais que bem intencionado que estivesse falhou ao tentar julgar os crimes utilizando a analogia, vez que encontrava barreiras na Constituição Federal e ainda não encontrava nenhum auxilio por parte do legislativo no tocante a rever normas, ou permitir uma interpretação mais extensiva de seus artigos.

Diante de toda essa nova modalidade delituosa ficou notória a necessidade da criação de uma Lei que regulamentasse esses atos, assim como ficou claro esse processo se deu de forma lenta e burocrática, ficando evidente o descaso do judiciário frente a várias Leis que tramitavam a muito tempo e foram simplesmente deixadas e lado após o episódio aclamado pela mídia quando fotos intimas da atriz Carolina Dieckmann foram espalhadas pela *internet*, fazendo assim com que a Lei fosse elaborada e sancionada de forma célere deixando muitas lacunas a serem preenchidas, por não ter sido analisada de forma devida e atendendo apenas ao grande clamor da mídia esquecendo-se de que as Leis são feitas para garantir a segurança e a integridade de todas as pessoas.

Diante de tudo isso, a melhor solução para o problema gerado é o usuário do equipamento eletrônico e da internet, se proteger por conta própria criando barreiras para que seus dispositivos não sejam invadidos e ficando sempre atento a golpes e as paginas de *internet* que acessa, assim como, cabe ao governo investir mais na capacitação de seus agentes e na compra de equipamentos, para que a Lei em estudo possa ser cumprida de maneira eficiente.

REFERÊNCIAS

BRITO, A. **Análise da Lei 12.737/12 – "Lei Carolina Dieckmann"**, 2013. Disponível em: http://atualidadesdodireito.com.br/aurineybrito/2013/04/03/analise-da-lei-12-73712-lei-carolina-dieckmann/ [Acesso em: 13 de novembro de 2013].

CAPEZ, F., **Curso de Direito Penal**, volume 2: parte especial, arts. 121 a 212. – 13° edição de acordo com as Leis n° 12.720 e 12.737, de 2012 – São Paulo. Editora Saraiva, 2013, p:424 e 425.

BRASIL, **Código Penal: promulgado em 7 de dezembro de 1940. Lei Nº 12.735, de 30 de novembro de 2012.** Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm [Acesso em: 13 de novembro de 2013].

BRASIL, **Código Penal: promulgado em 7 de dezembro de 1940. Lei Nº 12.737, de 30 de novembro de 2012**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm [Acesso em: 13 de novembro de 2013].

BRASIL, **Código Penal: Decreto-Lei N°2848, promulgado em 7 de dezembro de 1940**. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm [acesso em: 13 de novembro de 2013].

CABETTE, E.L.S. **O Novo Crime de Invasão de Dispositivo Informático**. 2013. Disponível em: http://www.conjur.com.br/2013-fev-04/eduardo-cabette-crime-invasao-dispositivo-informatico [Acesso em 02 de maio de 2014].

CONVERGÊNCIA DIGITAL, **Crimes Cibernéticos: Lei Carolina Dieckmann é sancionada sem vetos**, 2012. Disponível em http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=32532&sid=18#.UokWsnCmigS [Acesso em: 10 de novembro de 2013].

CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL: promulgada em 5 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao [Acesso em: 08 de novembro de 2013].'

JUNIOR RAMOS, H.S. **Invasão de Dispositivo Informático e a Lei 12.737/12: Comentários ao art. 154-A do Código Penal Brasileiro**. Simpósio Argentino de Informatica y Derecho, SID 2013. Disponível em: http://www.42jaiio.org.ar/proceedings/simposios/Trabajos/SID/09.pdf [Acesso em: 02 de maio de 2014].

MAGIC WEB DESIGN, **O que muda com a "Lei Carolina Dieckmann?"**, 2011. Disponível em: http://www.magicwebdesign.com.br/blog/lei-carolina-dieckmann/ [Acesso em: 10 de novembro de 2013].

OLIVEIRA, M.E., **ORKUT: O Impacto da Realidade da Infidelidade Virtual**, Rio de Janeiro, 2007. Disponível em: http://www.maxwell.lambda.ele.puc-rio.br/9888/9888_1.PDF [Acesso em: 08 de novembro de 2013].

PRADO, L.R., **Curso de direito penal brasileiro**, volume 2: parte especial, arts.121 a 249/ Luis Regis Prado. – 11° ed. ver. atual. e ampl. – São Paulo: Editora Revistas dos Tribunais, 2013. p:406.

SILVA, A.K.C. **O estudo comparado dos crimes cibernéticos: uma abordagem instrumentalista-constitucional acerca da sua produção probatória em contraponto à jurisprudência contemporânea brasileira**. Disponível em: http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=9962&revista_caderno=17 [Acesso em: 02 de maio de 2014].

SUA PESQUISA, **História da Internet**, 2012. Disponível em: http://www.suapesquisa.com/internet/ [Acesso em: 08 de novembro de 2013].

VICENTIN, T. **Lei Carolina Dieckmann não irá intimidar cibercriminosos**. 2013. Disponível em: http://idgnow.uol.com.br/internet/2013/04/03/lei-carolina-dieckmann-nao-ira-intimidar-cibercriminosos-diz-expert/ [Acesso em 13 de novembro de 2013].

CABETTE, E.L.S. O Novo Crime de Invasão de Dispositivo Informático. 2013. Disponível em: http://www.conjur.com.br/2013-fev-04/eduardo-cabette-crime-invasao-dispositivo-informatico [Acesso em 02 de maio de 2014].