UNIVERSIDADE TIRADENTES - UNIT

CURSO DE GRADUAÇÃO EM DIREITO

TRABALHO DE CONCLUSÃO DE CURSO – ARTIGO CIENTÍFICO

CIBERCRIMES: Desafios e perspectivas da legislação brasileira

Camila Cordeiro Vieira

Grasielle Borges Vieira de Carvalho

Aracaju

2015

CAMILA CORDEIRO VIEIRA

CIBERCRIMES: Desafios e perspectivas da legislação brasileira

Trabalho de Conclusão de Curso – Artigo – apresentado ao Curso de Direito da Universidade Tiradentes – UNIT, como requisito parcial para obtenção do grau de bacharel em Direito.

Aprovado em 30 / 05 / 2015 .

Banca Examinadora

Grasielle Borges Vieira de Carvalho
Professor Orientador
Universidade Tiradentes

Eduardo Torres Roberti
Professor Examinador
Universidade Tiradentes

Júlio César do Nascimento Rabelo
Professor Examinador
Universidade Tiradentes

CIBERCRIMES: Desafios e perspectivas da legislação brasileira

Camila Cordeiro Vieira [1]

RESUMO

O presente estudo tem como finalidade discorrer acerca da Lei 12.737/2012 (popularmente conhecida como "Lei Carolina Dieckmann"), que acrescentou dispositivos legais a fim de tipificar os delitos cibernéticos. Partindo-se da premissa de que a criação da lei preencheu uma lacuna na legislação brasileira acerca do tema, fica patente que houve um avanço considerável no quesito de segurança no mundo virtual em nosso ordenamento jurídico. E por esse caminho, objetiva-se compreender todo o processo de elaboração de dispositivos em combate ao Cibercrime. Inicia-se na análise de projetos de lei e comparativos com diplomas legais de outros países, bem como a visão jurisprudencial e doutrinária, visando destrinchar o seu conteúdo e trazer informação à sociedade que se encontra imersa no mundo virtual. Por fim, o estudo em tela irá traçar as perspectivas trazidas com o novo diploma legal e as mudanças para os usuários da rede mundial de computadores.

Palavras-chave: Cibercrimes. Lei 12.737/2012. Lei Carolina Dieckmann.

1 INTRODUÇÃO

Com o avanço da tecnologia, é raro encontrar alguém que não faça uso de pelo menos um apetrecho tecnológico que tenha acesso à internet e, consequentemente, às redes sociais, que são a verdadeira febre da sociedade moderna. As também chamadas "mídias sociais", para os mais técnicos, fazem parte do cotidiano e já não se pode imaginar a vida sem elas.

Ocorre que assim como na vida real, não estamos totalmente protegidos dos perigos que nos cercam no mundo virtual. Isso porque a célebre janelinha de oportunidades acaba se tornando um portal de acesso direto à vida da população, que por estar tão conectada, acaba incorporando a vida real à virtual, tornando seus dados expostos e acessíveis em apenas um clique.

Por ser precária a legislação que atua como meio de punibilidade pelo Estado, a criminalidade avançou mais rapidamente do que nosso ordenamento jurídico no tocante ao tema, de forma que as condutas estão muito sofisticadas enquanto que e as técnicas para se chegar ao autor do crime ainda estão em fase de aprimoramento, o que gera uma situação de impunidade na comunidade cibernética.

Diante de tal fato, a legislação pátria faz uso de analogias e jurisprudências para diversos casos de crimes cibernéticos, e passou por considerável avanço no sentido de se adequar a essa nova tendência mundial, com a promulgação da Lei 12.737 de 30 de novembro de 2012, que trouxe como inovação para o ordenamento jurídico o crime de "Invasão de Dispositivo Informático", que torna crime a conduta de invadir dispositivo informático alheio com o intuito de obter vantagem ilícita.

Vale ressaltar que a legislação em questão acabou ganhando o apelido de "Lei Carolina Dieckmann", nome da atriz da Rede Globo de Televisão que foi vítima de invasão de computador, onde imagens contidas em seu aparelho foram utilizadas como meio de extorsão e posteriormente divulgadas, e tal episódio acelerou o andamento de projetos que já tramitavam com o fim de regulamentar essas práticas delitivas cometidas em meios informáticos para modernização do Código Penal Brasileiro.

É certo que com a criação dessa disciplina normativa no Brasil, muitas questões abrolharam na mente de todos aqueles que se debruçam sobre o tema. Deste modo, o presente trabalho terá por ponto de maior relevância não somente fazer uma simples análise da lei e sua aplicabilidade, mas contribuir com o esclarecimento das dúvidas da sociedade em relação a eventuais questões e buscar soluções para algumas destas.

Conforme aduziu-se anteriormente, o método de abordagem escolhido para o trabalho será o dialético, vez que este tipo de pesquisa tem a finalidade de explicar e identificar os fatores causadores de tais fenômenos. O método auxiliar será o histórico, onde diante dos dados colhidos ao longo da história da internet, será feito um estudo de como se desenvolveram os cibercrimes ao longo da história, chegando aos dias atuais. Quanto aos objetivos, o método de abordagem será o qualiquantitativo, onde a análise estatística e investigação de dados serão de suma importância a elaboração das soluções para as questões norteadoras.

As técnicas empregadas serão a pesquisa bibliográfica, abordando a doutrina e jurisprudência, bem como a própria legislação, além da pesquisa documental de campo, tendo

em vista que a coleta de dados será feita com vítimas de crimes cibernéticos, sendo todas as fontes de suma importância para a conclusão deste trabalho.

2 DO CIBERCRIME: O CRIME SAI DAS RUAS E GANHA A TELA DO COMPUTADOR

Inicialmente, aborda-se a figura do cibercrime, indo desde o surgimento desse termo comumente usado na sociedade atual, onde se integram o mundo real e o mundo virtual, ambos tão opostos e paradoxalmente, conexos.

Será compreendido através de uma linha do tempo traçada a partir dos primórdios da internet que, com o passar dos anos, fez a rede mundial de computadores interagir de maneira mais frequente no cotidiano oferecendo infinitos benefícios aos seus usuários.

2.1 Breve histórico da internet: O "mundo cibernético"

Com o fenômeno da globalização, a humanidade tem passado por constantes transformações, sobretudo no que diz respeito à tecnologia, nas últimas décadas. Motivados pela praticidade de envio e recepção de informações, o homem e a máquina por ele criada estão cada vez mais sintonizados.

A praticidade é tamanha que muitas atividades antes feitas de maneira artesanal e manual agora são feitas através de máquinas comandadas por um único toque. O homem moderno é aquele que cria e aperfeiçoa a tecnologia para posteriormente desfrutar de todos os benefícios que uma máquina pode lhe oferecer.

Com a criação do computador, o termo "Cibernético" tornou-se cada vez mais popular. 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". Ora, tudo que for "Cibernético" é diretamente interligado com um mundo virtual, um "ciberespaço".

O próximo passo foi a criação da internet, que consiste em uma rede de computadores interligados como uma teia, onde informações são trocadas simultaneamente. A interação homem e máquina transformou-se de um modo até então imaginável apenas como roteiro de ficção e prova disso é a comunicação instantânea, que encurtou as distâncias e foi uma

maneira de acelerar o processo de globalização, quando o computador passou a ser ferramenta indispensável para a elaboração de uma miscelânea de atividades e adentrou as casas.

Datado de 1839, o primeiro protótipo de computador da história seria basicamente uma calculadora, uma máquina de calcular bastante rudimentar, de Charles Barbbage, "no qual o uso de cartões perfurados permitia a realização de cálculos matemáticos", conforme preleciona Maciel Colli. (2010, p. 31 Apud WINEGRAND et al 1996).

Partindo desse simples protótipo, ficou provado que o uso de determinados mecanismos tecnológicos seria um meio importante de desenvolvimento industrial, financeiro e social e tão logo a imagem de máquinas aliadas ao ser humano passou a ser bastante atrativa.

Os estudos e pesquisas começaram a ser aprimorados, de modo que o computador agora já fazia acompanhamentos biológicos da vida humana através de informações que eram inseridas nas máquinas e codificadas pelos sistemas mundo afora, gerando confiança nos sistemas e acreditando-se piamente na sua infalibilidade, devido a sua possibilidade mínima de erros.

A partir daí, aproximadamente por volta de 1960 o governo dos Estados Unidos iniciou um promissor projeto de pesquisa voltado ao aprimoramento de sua rede de computadores, denominado "Arpanet" (Agência de Pesquisa Avançada e Rede), como meio de internalizar suas comunicações para preveni-los em estado de guerra, por exemplo, sendo utilizada inicialmente como arma bélica. Assim surgiu a internet, que em transformação constante atingiu novos patamares e em 1973 já se fornecia meios de conexão entre usuários de computadores distintos, através de um código de modo que eles pudessem se comunicar.

Com mais mudanças, resta afirmado que o grande impulso da internet ocorreu na década de 1990, tornando uma ferramenta que aos poucos ganhou espaço e tornou-se indispensável no dia-a-dia, surgindo assim um novo ambiente que merece regulação como outros grandes meios de comunicação.

Com essa confiança entre homem e máquina estabelecida, diz-se que o homem estaria para a máquina como um comandante estaria a bordo de um navio em movimento, conduzindo-o e navegando nas águas do mundo virtual, coletando e inserindo dados de maneira frenética e constante.

2.2 Influência do mundo virtual no mundo real e a incidência dos crimes virtuais

Conforme mencionado anteriormente, as máquinas e o mundo virtual passaram a ter cada vez mais confiança do homem, de modo que tarefas mais relevantes começaram a ser executadas através da rede de sistemas operacionais. Bens essenciais ao homem contemporâneo como saúde, segurança, intimidade e propriedade, subjetiva ou objetivamente falando, puderam ser resguardados também através de bancos de dados, por exemplo.

Bancos de dados são meios de armazenamento de arquivos físicos que podem ser digitalizados ou virtuais, os quais podem ser modificados constantemente de maneira programada ou manual, estando sempre atualizados.

A informática e a internet, portanto, são imprescindíveis para a sociedade moderna, não se pode negar. Nesse ponto, por exemplo, é inimaginável pensar num retrocesso das agências bancárias e seu sistema financeiro que se dá basicamente através de processamento de dados feito eletronicamente.

Outro exemplo de como a tecnologia é importante para salvaguardar os benefícios inerentes à pessoa humana está na urna eletrônica utilizada durante as eleições gerais e municipais em todo o país. Consideradas como as mais democráticas e eficientes do mundo, as eleições realizadas por meio da urna eletrônica garantem maior segurança, além de assegurar os direitos de liberdade e democracia para os eleitores, causando enorme revolução Brasil afora e elevando o país a nível internacional de desenvolvimento no que diz respeito ao tema.

A propósito, o uso da tecnologia também se faz presente em meio ao Poder Judiciário no que diz respeito à recente virtualização dos processos, garantindo maior celeridade processual, organização e evitando os enormes arquivos históricos à exemplo do arquivo do Poder Judiciário do Estado de São Paulo, onde uma empresa terceirizada pelo Tribunal de Justiça do mesmo estado conta com um acervo com 58 milhões de autos processuais que tramitaram no TJ/SP desde 1781, não podendo ser visitados pelo público e logo, não podendo ser retirados sem criteriosa autorização.

Ademais, no que tange os conhecimentos tecnológicos de maneira pessoal, estes se fazem de grande valia no mercado profissional, uma vez que é indispensável para o homem saber manipular as tecnologias das mais simples, utilizadas hodiernamente até os mais sofisticados, que acrescentam um grau a mais no curriculum do individuo.

Contudo, assim como há avanço e benefícios diante dessa informatização atrelada à tecnologia, não é de hoje que pessoas se aproveitam dessa ferramenta para a prática de crimes.

Crimes estes que não somente fazem parte do cotidiano como são aprimorados constantemente, acompanhando a evolução digital.

Pesquisas demonstram que o universo dos crimes informáticos de fato acompanhou o crescimento da era digital e teve seus os primeiros indícios no século XX, mais precisamente em 1960, quando ainda estava sendo descoberta e aprimorada a tecnologia em questão, as primeiras modalidades de crimes nas mais diversas denominações tiveram seus primeiros casos de manipulação e sabotagem de sistemas de computadores e por volta da década de 70 a figura do Hacker já era citada com o advento de crimes como invasão de sistema e furto de software.

No entanto, na década de 1980 houve a maior propagação dos diferentes tipos de crimes tais como a pirataria, pedofilia, invasão de sistemas, propagação de vírus, acendendo a luz de alerta sobre os riscos de se expor informações no mundo virtual, e a partir pesquisas na área de desenvolvimento ocorreram de forma atrelada à meios de cuidados com a segurança virtual, exigindo uma atenção especial para identificação e punição dos responsáveis, cientes de que a essa altura estão em todos os lugares do mundo, uma vez que os criminosos acompanharam a evolução tecnológica.

Com a chegada dos computadores e acesso à internet em massa, o Brasil começou a se preocupar com esse assunto especialmente a partir das últimas décadas, com o aumento da popularização dessa inovação tecnológica, promulgando, na Constituição Federal de 1988, leis relativas à competência do Estado sobre questões de informática e automação (MONTEIRO, 2014).

É válido ressaltar que a Carta Magna apesar de tão atual, não acompanhou o processo de atualização do mundo virtual e consequentemente, seus crimes. Ou seja, por mais que se tenha dispositivos legais que mencionam a garantia da segurança das informações, eles não são suficientes para atender a demanda de uma infinidade de ameaças que cercam os usuários todos os dias e atualizam-se constantemente, indo de encontro ao direito que, lamentavelmente, é tão estático.

Convém salientar que o atual Código Penal, por exemplo, é datado da década de 1940, onde o meio de comunicação mais expressivo era o rádio e onde claramente podemos perceber que as nossas leis não acompanharam o processo de desenvolvimento tecnológico.

Dessa forma, se entende que os crimes habituais relacionados à informática que estão previstos na legislação atual não são suficientes para classificar os crimes cometidos contra o

computador ou por meio dele frente às novas modalidades criminosas que surgiram e que merecem ser definidos em lei especial, para garantia da ordem legal.

Em uma rápida pesquisa através de sites de pesquisa é possível encontrar diversos significados para os crimes cometidos por meio da internet. Constata-se que os cibercrimes consistem em múltiplas condutas que podem ser praticadas de modo reiterado ou não, em concurso de agentes ou não, utilizando-se de meios que vão além do mundo virtual, ou não. Ou seja, é possível compreender que há uma gama muito ampla de condutas assim como há infinitos modos de operá-las, devendo haver diferentes maneiras para solucionar cada um deles.

Por ser complexo conceituar o crime, mais ainda o é para identificar o criminoso, uma vez que esse se aproveita do falso anonimato que se tem por estar diante de uma tela e mais ainda, da ingenuidade daqueles com pouco conhecimento tecnológico que por muitas vezes crê piamente que não há meios de se chegar ao agressor.

Ademais, por falta de legislação específica que trate dos delitos virtuais em sua totalidade os juristas acabam por aplicar certa analogia no Direito Penal (que, via de regra, não pode existir: *"nullum crimen nulla poena sine lege stricta"*), utilizando como parâmetro o crime semelhante existente no ordenamento jurídico para punir crimes e fixar penas aos delitos virtuais, e que conforme o entendimento do presente artigo e a ideia de dever ser preservada a função integradora dos princípios, vez que é verdadeira função da norma quando aplicada ao caso concreto.

É válido esclarecer que embora seja permitida a interpretação da norma processual penal de forma extensiva, crimes cibernéticos vão além da previsibilidade do direito processual penal, e acabam por impedir uma persecução penal eficaz, tal qual a aplicação de medidas paliativas por falta de medidas específicas.

As afirmações acima mencionadas possuem respaldo para seu fundamento conforme demonstrado na jurisprudência brasileira, da Quinta Turma do Superior Tribunal de Justiça (STJ):

> CRIMINAL. HC. FURTO QUALIFICADO. FRAUDES POR MEIO DA INTERNET. PROGRAMA TROJAN. OPERAÇÃO CONTROL ALT DEL. PRISÃO PREVENTIVA. POSSIBILIDADE CONCRETA DE REITERAÇÃO CRIMINOSA. NECESSIDADE DA CUSTÓDIA DEMONSTRADA. PRESENÇA DOS REQUISITOS AUTORIZADORES. ORDEM DENEGADA. Hipótese na qual o paciente foi denunciado pela suposta prática do crime de furto qualificado, pois seria integrante de grupo

> organizado com o fim de praticar fraudes por meio da Internet, concernentes na subtração de valores de contas bancárias, em detrimento de diversas vítimas e instituições financeiras, entre elas a Caixa Econômica Federal, a partir da utilização de programa de computador denominado TROJAN. Não há ilegalidade na decretação da custódia cautelar do paciente, tampouco no acórdão confirmatório da segregação, pois a fundamentação encontra amparo nos termos do art. 312 do Código de Processo Penal e na jurisprudência dominante. As peculiaridades concretas das práticas supostamente criminosas revelam que a liberdade do réu poderia ensejar, facilmente, a reiteração da atividade delitiva, indicando a necessidade de manutenção da custódia cautelar. As eventuais fraudes podem ser perpetradas na privacidade da residência, dos escritórios ou, sem muita dificuldade, em qualquer lugar em que se possa ter acesso à rede mundial de computadores. A real possibilidade de reiteração criminosa, constatada pelas evidências concretas do caso em tela, é suficiente para fundamentar a segregação do paciente para garantia da ordem pública. Ordem denegada.
>
> (STJ - HC: 81638 PA 2007/0087811-8, Relator: Ministro GILSON DIPP, Data de Julgamento: 12/06/2007, T5 - QUINTA TURMA, Data de Publicação: DJ 06.08.2007 p. 598)

Restou demonstrado que algumas modalidades de práticas delituosas por meio da internet ocorrem contra instituições financeiras e seus usuários, através de programas de computador que podem ter acesso ao sistema de instituições e vítimas de qualquer lugar do país sem nenhum fator impeditivo para os criminosos.

A prática delituosa por meio virtual não está resumida apenas em fraudes, estelionato e furto de dados bancários, essa é apenas a "ponta do iceberg". Crimes contra a pessoa como calúnia, difamação e injúria também ocorrem na rede e a dificuldade de punir os agentes causadores se torna ainda maior devido a escassez de preparo técnico e recursos para a investigação de tais atos, conforme demonstrado na jurisprudência da Turma Recursal Criminal dos Juizados Especiais Criminais do Estado do Rio Grande do Sul:

> "APELAÇÃO – CRIME- QUEIXA-CRIME – ARTS. 139 E 140 AMBOS DO CÓDIGO PENAL – OFENSAS PELO ORKUT – AUTORIA INCONCLUSIVA.

> (...) Ocorre que para a demonstração efetiva da autoria deveria ser trazida aos autos prova técnica capaz de demonstrar tenham as mensagens se originado do computador utilizado pelo apelado, ou ainda, informações do ORKUT, via acesso a banco de dados, esclarecendo a origem das mensagens pejorativas, identificando e localizando o computador de onde partiram estas mensagens, o que inocorreu."

Fica patente que, devido aos argumentos trazidos e comprovados mediante decisão proferida, resta ao cidadão lesado através o prejuízo na elucidação dos fatos e a impunidade para tais condutas, que continuam a ser praticadas livremente sem a devida punição.

Apesar disso, há esperança advinda de uma reciclagem em nossa legislação com o enfoque, também, nos crimes cibernéticos. Com debates acerca da criação do novo Código Penal, crimes "modernos" ganharão tipificação na lei e prometem maior fiscalização e punição aos agentes de condutas delituosas.

3 EVOLUÇÃO ACERCA DOS CRIMES CIBERNÉTICOS: HISTÓRICO DOS PROJETOS DE LEI

Com a exposição massiva a que o homem está sujeito diariamente seja por meio físico ou virtual, resta provado que o direito necessita estar em constante movimento, acompanhando tais mudanças, a fim de resguardar das ameaças da contemporaneidade e para isso caminha em direção a uma nova vertente: O Direito da Informática.

Cumpre observar que a influência da informática já avançou significativamente quando o legislador atentou para isso ao menos em esfera cível na criação do Código Civil de 2002, no que tange o comércio eletrônico e, além disso, na estipulação de contratos, onde é cabível a conceituação de um negócio jurídico que para ser validado depende da exteriorização de vontade das partes, requisito que está sendo perfeitamente aplicado nos contratos eletrônicos. O mesmo pode-se observar no Código de Defesa do Consumidor, onde a internet é aliada de empresas na divulgação em massa visando atrair novos consumidores.

É válido ressaltar também a presença da internet e da informática junto ao Código de Processo Civil, uma vez que atualmente, nas execuções, permite-se a penhora online, onde através do "Bacen-Jud" o juízo da execução tem a possibilidade de obter informações sobre depósitos bancários, por exemplo, do executado realizados em qualquer instituição financeira

de qualquer localidade do país. Com isso, o magistrado tem maior autonomia para poder determinar o bloqueio do valor do crédito do executado, de modo a concretizar o direito do exequente quando da penhora de dinheiro.

Acompanhando a crescente modernização do poder judiciário e da legislação pátria, em tempo a inovação também repercutiu, ainda que de maneira lenta, no Direito Penal e Processual Penal, onde se confere que até meados de 2012 a internet era isenta de qualquer legislação específica e em virtude disso, a realização de crimes e condutas lesivas se tornou um verdadeiro parasita na vida dos usuários.

Como restará demonstrado à seguir, o problema da falta de legislação penal já começou a ser analisado e trazido para discussão na bancada do legislador, uma vez que, em tempo, o mesmo atentou para o fato de que o Direito Penal não aplica analogias em virtude do princípio da legalidade, presente em nossa Constituição Federal em seu art. 5º, inciso XXXIX - "Não há pena sem lei anterior que o defina, nem pena sem prévia cominação legal" - e, assim, muitos crimes virtuais na esfera penal acabaram sem a punição devida aos infratores.

3.1 Do Do PL 84/1999 (PL 89/2003) e a Lei 12.735

Como objeto de estudo deste trabalho, será abordado sobre a Lei 12.737/2012, que deu ensejo a modificações relevantes no Código Penal acerca do mundo virtual. Porém, antes disso, outros projetos de lei no cenário nacional na tentativa de dirimir tais condutas.

Iniciando os debates acerca do tema, o Projeto de Lei nº 84 de 1999, onde o relator foi o Deputado Eduardo Azeredo e, popularmente chamado de Projeto Azeredo, o referido projeto discutia acerca da problemática dos crimes virtuais ainda que de maneira tímida, abordando condutas como acesso não autorizado mediante quebra de dispositivo de segurança, cópia de senhas ou outras informações pessoais, "pishing" ou estelionato eletrônico, ataques a redes de computadores, clonagem de cartões de crédito e os mesmos crimes quando praticados por militares. Ainda no projeto, discutiu-se a pena de 1 a 3 anos e dobrada, caso comprovado que o usuário disponibilizou material com conteúdo protegido por direitos autorais, tais como vídeos, seriados e músicas.

De modo acanhado, mas importante, o PL 84/1999 foi o marco inicial na tipificação de condutas cometidas por meios virtuais. Em abril de 2013, o PL foi sancionado como lei e modificou o Código Penal para tornar crime a clonagem de cartões de crédito ou débito,

equiparando este delito à falsificação de documentos particulares, tipificado no art. 155, §2, II do C; além de determinar que órgãos da polícia judiciária criem delegacias especializadas.

Fica destacado que o PL 89/2003, outra importante iniciativa no trato dos crimes virtuais, onde visa coibir a prática de crimes como a pedofilia, disseminação de vírus, criminalizar o roubo de senhas dentre outras condutas.

Esse projeto chegou a tramitar por vários anos no Congresso Nacional e teve sua redação final aprovada pelo Senado somente em 2008, com caráter substitutivo ao PL 84/1999. Mencionado projeto, todavia, desencadeou intensos embates jurídicos sobre o seu conteúdo e inclusive recebeu incontáveis críticas dos internautas ativistas que, conforme apontou o jornal câmara vinculado a Câmara dos Deputados, chegou a circular uma petição contrária à aprovação deste projeto com mais de 165 mil assinaturas. Por esse motivo, o projeto ficou conhecido como "AI-5 Digital", visto que era tão rigoroso que suprimia a liberdade de expressão dos internautas e os enquadraria na tipificação penal um simples download, por exemplo.

Essa falha no projeto foi discutida inclusive pelo Centro de Tecnologia e Sociedade da Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas, onde em artigo publicado em agosto de 2008, comentários foram tecidos acerca das possíveis falhas e melhorias a serem feitas no intuito de viabilizar o projeto, pois em outras palavras, se fosse aprovado da forma como estava, o projeto levaria à criminalização potencial de um elevado número de usuários pela prática de atos que em sua maioria são legais ou ainda, regulados como ilícitos civis em função do seu menor potencial ofensivo.

Segundo Jôline Cristina de Oliveira, era patente a falta de critérios capazes de distinguir o uso mais correto da tecnologia das agressões sofridas no universo informático, e por isso aduz que:

> "O projeto de lei pecava pela subjetividade das normas abertas ou especificações atécnicas utilizadas para caracterizar as ações. (...) Tratava-se em verdade, de uma tentativa tênue e crua de resguardar novos valores, os quais a sociedade brasileira passava a eleger na medida em que ia aumentando sua dependência em relação a eles".

Ainda neste tocante, aduz que justamente por ser considerado obsoleto e prolixo,

> "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". (OLIVEIRA, 2013, 18- 22)

3.2 O PL 2.793/2011 e a Lei 12.737

O Projeto de Lei nº 2.793 de 2011, de autoria da deputada Manuela D'Ávila (PCdoB/RS) e dos deputados Paulo Teixeira (PT/SP), Luiza Erundina (PSB/SP), João Arruda (PMDB/PR), Brizola Neto (PDT/RJ) e Emiliano José (PT/BA) que versava dos crimes cometidos na internet foi a mola precursora para a atual Lei Carolina Dieckmann – L.12.737/12.

Na época, em maio de 2012, os autores alegavam que "são inegáveis os avanços para a sociedade decorrente do uso da Internet e das novas tecnologias". Ademais, diziam que "tais avanços trazem a necessidade da regulamentação de aspectos relativos à sociedade da informação, com o intuito de assegurar os direitos dos cidadãos e garantir que a utilização destas tecnologias possa ser potencializada em seus efeitos positivos e minimizada em seus impactos negativos".

Do ponto de vista prático, houve alterações singelas nos artigos 154 e 155 do Código Penal vigente, onde para o crime de "devassar dispositivo informático alheio" com o objetivo de mudar ou destruir dados ou informações, instalar vulnerabilidades ou obter vantagem ilícita, o texto atribui pena de três a um ano de detenção e multa.

Ademais, pelo projeto seria enquadrado no mesmo crime aquele que produzisse, oferecesse, distribuísse, vendesse ou difundisse programa de computador destinado a permitir o crime de invasão de computadores ou de dispositivos como smartphone e tablet.

Haveria aumento de pena de 1/6 a 1/3 se a invasão resultasse em prejuízo econômico; e de 1/3 à metade se o crime fosse praticado contra o Presidente da República, governadores e prefeitos; presidente do Supremo Tribunal Federal; e presidentes da Câmara dos Deputados, do Senado, de Assembleia Legislativa de estado, da Câmara Legislativa do Distrito Federal ou de Câmara de Vereadores.

Com a aprovação do PL 2.793/2011 foi permitido o desapensamento de itens desnecessários contidos nos projetos anteriores, sendo de fato mais proveitoso para a sociedade como defendiam os autores, tendo em vista que continha poucas disposições legais sobres os cibercrimes ao ser comparado com o já mencionado Projeto de Lei n. 89/2003.

Conforme pesquisado, os autores argumentavam que boa parte dos delitos já praticados com o auxílio ou não da internet implicam numa repressão que já está contida no ordenamento jurídico, e de tal modo foram tipificados apenas delitos que violavam certo bem jurídico onde não havia cominação legal.

Diante de tantas críticas, o projeto de lei nº 2.793/11 fora apensado e desapensado a outros projetos por diversas vezes, sendo desengavetado apenas posteriormente, quando fora aprovado sob as críticas do deputado Eduardo Azeredo (PSDB/MG), relator do PL 84/1999 e 89/2003, que denunciou o casuísmo do governo.

Azeredo afirmava que o governo era omisso acerca do tema, onde o debate já havia sido iniciado há anos que o novo projeto foi aprovado logo após o vazamento de fotos íntimas da atriz Carolina Dieckmann.

De fato, a problemática que circundava os projetos de lei só teve fim com o episódio envolvendo a atriz global, que foi vítima de crackers que se aproveitaram da falta de dispositivos de segurança contra vírus e spams em seu computador, obtiveram a senha do seu e-mail e encontraram nele diversas fotos da atriz seminua e em posições em que expunha sua intimidade. Tais fotos foram disseminadas aquém dos delinquentes, que as divulgaram inclusive em sites pornográficos.

Após a grande repercussão, os agentes criminosos foram localizados, presos e juntamente com eles foram apreendidos os computadores e demais instrumentos do crime. Em meio a suas condutas, tais agentes foram indiciados pelo crime de furto, o que a nosso ver, corresponde analogicamente ao tema vez que nosso ordenamento não possuía a época a legislação adequada para o tipo penal.

A partir de então, nasceu a Lei 12. 737/2012. As alterações que a Lei trouxe estão presentes nos arts. 154-A e 154-B do Código Penal Brasileiro, onde torna crime a invasão de dispositivo informático e quanto à ação penal, esta 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.

Também ocorreu a inclusão dos parágrafos 1º e 2º ao Art. 266, onde incorre na mesma pena do delito de interrupção de serviço telegráfico, radiográfico e telefônico a conduta que interrompa serviço telemático ou de informação de utilidade pública, a qual deverá ser dobrada em ocasião de calamidade pública.

Ademais, está presente a modificação do Art. 298, para a inclusão do parágrafo único que define o crime de falsificação de cartão de crédito. Desta forma, o cartão de crédito ou débito fica equiparado a documento particular. (OLIVEIRA, 2013, 23).

4 A LEGISLAÇÃO AO REDOR DO MUNDO

A necessidade de criar no ordenamento jurídico uma legislação própria acerca dos crimes virtuais deixou de ser algo acessório para se tornar principal, como pôde ser visto nos tópicos anteriores.

Logo, a ideia de coibir os delitos praticados com as leis já existentes caiu por terra quando se verificou que a modernidade e seus avanços tecnológicos haviam atingido um patamar superior, criando conceitos próprios e que não mais poderiam ser interpretados com os tipos penais preexistentes.

4.1 A Convenção de Budapeste

É dito popularmente que "no Brasil, existe lei para tudo", no entanto dentro desse vasto arcabouço jurídico muitas de nossas leis estão obsoletas, e diante dessa problemática estavam os crimes cibernéticos que fazem parte do cotidiano e crescem assustadoramente, de maneira que o legislador precisa se atualizar e acompanhar esse processo.

Neste tocante foi criada no ano de 2001 na Hungria, através do Conselho da Europa, a Convenção sobre o Cibercrime ou popularmente conhecida como a Convenção de Budapeste, a qual engloba mais de 20 países tipifica os principais crimes cometidos na Internet e está em vigor desde meados de 2004, após ser ratificada por cinco países.

A Convenção possui quatro capítulos nomeados como: Terminologia, Medidas a Tomar a Nível Nacional, Cooperação Internacional e Disposições Finais, respectivamente, dispostos em 48 artigos. Ainda em sua finalidade inicial, ressalta o respeito à Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa (1950); ao Pacto Internacional sobre os Direitos Civis e Políticos da ONU (1966); à Convenção das Nações Unidas sobre os Direitos da Criança (1989); e à Convenção da Organização Internacional do Trabalho sobre as Piores Formas do Trabalho Infantil (1999). (SOUZA e PEREIRA, 2009).

Com um texto sucinto, de fácil entendimento e ainda assim bastante completo, o tratado define os cibercrimes, tipificando sua conduta, como infrações contra sistemas e dados informáticos, infrações relacionadas com computadores, infrações relacionadas com o conteúdo, pornografia infantil e infrações relacionadas com a violação de direitos autorais.

No momento em que foi ratificada a Convenção, no ano de 2004, no Brasil estava eclodindo a disputa do Projeto Azeredo que tramitaria por 10 anos no Congresso Nacional e que somente entraria de fato em vigor anos mais tarde, onde nesse lapso temporal o país não tinha qualquer legislação que abrangesse o tema de crimes virtuais.

Sucede que apesar da flexibilidade do texto do tratado no que tange a resolução dos conflitos, sendo uma boa alternativa para o país que se encontrava ainda sem nenhum norte no que se referia à tipificação dos delitos virtuais, o Brasil não fora um dos signatários do tratado não podendo simplesmente aderir à Convenção, tendo que ser convidado a participar por meio do Comitê de Ministros do Conselho Europeu, conforme texto original no art. 37, o qual aduz que: "(...) O Comitê de Ministros do Conselho da Europa pode (...) convidar qualquer Estado não membro do Conselho e que não tenha participado na sua elaboração, a aderir à presente Convenção" (CONVENÇÃO SOBRE O CIBERCRIME, p. 23).

Há de se lembrar que há anos corre a proposta de reforma do Código Penal de 1940 e com isso, muitos artigos serão alterados e outros tantos serão inseridos, inclusive no que diz respeito aos cibercrimes. Com muitas promessas e nada conclusivo, após longos anos de tramitação e com alterações feitas no PL 84/99, o país possui atualmente uma esperança de mudanças mais significativas no campo dos crimes virtuais além da promulgação da Lei 12.737/12.

Ocorre que a política de crimes cibernéticos já é pauta em outros países, e diante dessas informações torna cabível uma análise sobre as formas legislativas adotadas, assim como os seus mecanismos de coibição. Passemos, de fato, às análises:

4.1.1 Estados Unidos

É válido ressaltar que no Direito Penal norte-americano há duas modalidades de incriminação: a tipificação estatutária (o direito penal codificado como temos aqui no Brasil) e os ilícitos decorrentes de decisões judiciais, uma forma quase inexistente na atualidade. (SILVA, 2012)

Tendo por esse viés, o combate a crimes virtuais no pais se deu em dois patamares: o estadual e o federal. No âmbito federal encontrou-se a Lei de Proteção aos Sistemas Computacionais (Federal Computer System Protection Act of 1981), a qual determinava como conduta delituosa o uso de computadores com o objetivo de praticar fraudes, furtos ou espécies de apropriação indébita.

Em 1982 surgiu a Eletronic Funds Transfer Act, que trata da regulamentação de transferências eletrônicas de fundos, incriminando as fraudes informáticas que não continham relações interpessoais. (...) E a principal lei que aborda a responsabilização criminal de condutas ilícitas no âmbito informático é a Computer Fraud and Act (Lei de Fraude e Abuso Computacional) datada de 1986 que visa proteger a acessibilidade dos sistemas para a obtenção de segredos nacionais ou com o intuito de obter vantagens financeiras. (SILVA, 2012).

4.1.2 Alemanha

Tendo por base o processo penal inquisitivo inerente ao direito alemão, a investigação torna-se de suma importância no CPP, de modo que pelo princípio da investigação de ofício utiliza-se o Código de Processo Penal aliado à Lei Orgânica, pautando-se então a investigação dos crimes pelo Poder Público.

Aproximadamente na década de 80 o interesse em investigar e punir os cibercrimes, ainda que de pouca incidência e pouca relevância. Tanto que seus principais problemas na esfera tecnológica se referem ao uso abusivo de informações, onde em 1986 fora editada a Segunda Lei de Combate à Criminalidade Econômica, que traz em seu texto normas contra a criminalidade informática. Na presente legislação, não são punidas meras invasões de sistema, porém, alguns delitos são tipificados de forma especial como: espionagem de dados; extorsão informática; falsificação de elementos probatórios, incluindo aí a falsidade documental e a ideológica; sabotagem informática; alterações de dados e utilização abusiva de cheques ou cartão magnéticos.

4.1.3 França

Com características do sistema processual acusatório e inquisitivo, onde dependendo da gravidade do delito em questão, o juiz pode participar mais ativamente no que tange à fiscalização, bem como a polícia pode dar as cartas na investigação.

> "Via de regra, a França não apresenta legislação destinada a punição de condutas criminosas no âmbito digital, mas em 1988 o Código Penal sofreu algumas alterações e pela Lei n.88-19, acrescentando um capítulo especial elencando atentados contra sistemas informáticos, contendo as seguintes incriminações, incriminando tipos como acesso fraudulento a sistema de elaboração de dados (art. 462-2), considerando como delitos tanto o acesso ao sistema quanto manter-se conectado ilegalmente, aumentando-se a pena caso haja supressão ou modificação de dados, e alteração no funcionamento do sistema". (SILVA, 2012)

Outro exemplo seria a sabotagem informática, (art. 462-3), que pune a conduta de quem apaga ou falseia o funcionamento do sistema eletrônico. No tocante à destruição de dados (art. 462-4), o dispositivo responsabiliza aquele que, dolosamente, introduz dados em sistema ou, de qualquer forma, suprime ou modifica dados.

Por fim, aborda-se sobre a falsificação de documentos informatizados (462-5), que busca punir quem falsificar documentos informatizados com a intenção de causar prejuízo a outrem e o uso de documentos informatizados (462-6), que pune quem faz uso dos documentos falsos retromencionados. (SILVA, 2012).

Há de se frisar que, como bem menciona Freitas Crespo, a França foi um dos primeiros países a dispor de Legislação em sede de criminalidade informática pelo advento da Lei. N. 78-17, de 06 de janeiro de 1978 e que as condutas já incriminadas ali corroboram as disposições de diretrizes internacionais já adotadas, assim como em especial a Convenção de Budapeste.

Conforme foi possível observar, cada Estado a seu modo lida com o tema de acordo com a relevância e urgência em que os casos de delitos informáticos ocorrem e é de suma importância que cada nação acompanhe de perto e tome um posicionamento à respeito, com as medidas cabíveis de forma abrangente e eficaz.

5 LEI 12.737/12: O MARCO INICIAL

Conforme observado, foi longo o caminho percorrido para a criação dos dispositivos aqui analisados, onde à sua maneira, cada qual teve o condão de preencher o vazio normativo existente na legislação penal brasileira, que permitia a prática de atos nitidamente ilícitos, diante da ausência de tipificação normativa.

Diversas foram as maneiras empregadas na tentativa de 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 e ao mesmo tempo, cumprir os princípios que norteiam o Direito Penal Pátrio, como o da legalidade que determina a existência previa da lei em relação ao fato ocorrido – *nullum crimen nulla poena sine lege praevia*.

Nesta esteira, fica patente que a aprovação da Lei Carolina Dieckmann ocorreu como o marco inicial na temática da segurança da informação e neste ínterim é desejo comum que haja maior proteção à intimidade e liberdade individual com o resguardo dos dados pessoais disponibilizados em dispositivos informáticos, de modo que a utilização dos mecanismos

cibernéticos possa ser considerada, de fato, segura e que seus usuários não fiquem receosos ao disponibilizarem suas informações na rede.

Fica evidente que a inovação criminológica neste aspecto requer muito mais que um diploma legal regulamentando as condutas delituosas. A partir daí, tais crimes precisam ser enfrentados por um poder investigatório mais apurado, com um maior aparato tecnológico e intelectual, vez que muitos dos crimes cometidos na internet envolvem a atuação de agentes com aguçado conhecimento informático e assim, de nada vale uma lei que insira no ordenamento jurídico pátrio novos tipos penais ao Código Penal se o Poder Judiciário, Ministério Público e as polícias Civil e Federal não estejam empenhadas e preparadas tecnicamente na prevenção e repressão destes crimes.

Dentro das pesquisas realizadas foi apurado inclusive que, com o trabalho conjunto do Banco do Estado de Sergipe (BANESE) e a Secretaria de Segurança Pública de Sergipe (SSP/SE), Aracaju já conta com um núcleo de atendimento aos crimes cibernéticos, a Delegacia de Repressão aos Crimes Cibernéticos (DRCC), que fica localizada no Complexo Especializado de Polícia Civil, na Rua Laranjeiras, 960, centro da cidade.

A DRCC funciona no atendimento direto ao cidadão, como para as instituições prejudicadas por crimes virtuais, fraudes bancárias, pedofilia e crimes contra a honra. O delegado que deu início aos trabalhos, Alessandro Vieira, afirmou que todo o trabalho da DRCC funciona em parceria com a Delegacia de Apoio a Grupos Vulneráveis (DAGV), Centro de Operações Policiais Especiais (COPE), Polícia Militar e Civil de Sergipe e de outros estados, além da Polícia Federal.

Resta provado que a lei sozinha não produzirá a eficácia necessária já que depende de uma atuação conjunta dos órgãos mencionados, como uma força-tarefa, a fim de melhor regulamentá-la e a partir de investimento na criação das novas delegacias especializadas juntamente com o treinamento de policiais no tocante as investigações forenses, a atuação na investigação e solução de crimes torna-se mais eficaz.

6 CONSIDERAÇÕES FINAIS

Neste trabalho houve o intuito de tratar acerca da aplicabilidade da Lei 12.737/2012 nos crimes virtuais, trazendo uma reflexão acerca do tema desde o seu surgimento até o ponto atual, onde ainda há muito que se aperfeiçoar no decorrer do tempo.

É sabido que a lei em tela não possui o condão de extinguir os crimes cometidos na internet em consequência do rápido avanço tecnológico e social, porém neste aspecto ficou comprovado que os desafios e perspectivas da legislação brasileira estão à luz da certeza de que sendo o Direito o verdadeiro regulador da ordem na sociedade, cabe a ele também, acompanhar os avanços e atualizar o ordenamento jurídico para tipificar tais condutas e se adaptar aos desafios da atualidade.

As considerações demonstradas objetivam a prevenção de crimes virtuais, entendendo que o tema que vem tomando grande espaço no cotidiano, ressaltando que somente a observância do legislador não se faz suficiente, vez que uma vez criada, a lei deve ser aplicada da forma mais eficaz e célere possível e tal agilidade se dará também com a criação de setores da polícia judiciária especializada.

Ademais, há de se considerar que a pressão popular causada pela exposição midiática fez com que os projetos fossem votados e aprovados, demonstrando a deficiência do legislador ao lidar com o tema. De mais a mais, a população não quer mais ficar "à mercê" dos criminosos na internet, exigindo, portanto um posicionamento mais eficaz do legislativo sobre o problema.

Há de se considerar que o passo ainda que tímido foi dado, o legislador criou tipos informáticos próprios, com a tipificação do delito de invasão de dispositivo informático e em decorrência desse endurecimento legal, é esperado que o debate acerca do tema sempre se faça presente para que o usuário venha a ter mais tranquilidade ao realizar suas ações diárias sem que para tanto, precise se preocupar com a segurança dos seus dados, sua liberdade de agir, intimidade e privacidade.

REFERÊNCIAS BIBLIOGRÁFICAS

BARRETO, Ana Amélia Menna - **Crimes digitais: 10 anos discutindo um PL e aprovam outro** - Núcleo de Direito Pontocom. Disponível em: < http://www.nucleodedireito.com/crimes-digitais-10-anos-discutindo-um-pl-e-aprovam-outro/>. Acesso em: 01 de abr. de 2015.

BRASIL. **PL 2793/2011**. Disponível em: < http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=944218&filename=PL+2793/2011> Acesso em: 20 de nov. 2014.

BRASIL. **PLS 89/2003.** Disponível em: < http://www.senado.gov.br/atividade/Materia/detalhes.asp?p_cod_mate=63967> Acesso em: 20 de nov. 2014.

BRASIL.**DECRETO-LEI 2.848/40** Disponível em:< http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>; Acesso em: 19 de nov. de 2014.

BRASIL. **LEI 12.737/2012** Disponível em:< http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em: 18 de nov. de 2014.

BRASIL. MINISTÉRIO PÚBLICO FEDERAL - **Cibercrime: CCJI sugere adesão do Brasil à Convenção de Budapeste -** Disponível em: < http://ccji.pgr.mpf.gov.br/institucional/informes/cibercrime-ccji-sugere-adesao-do-brasil-a-convencao-de-budapeste >. Acesso em: 03 de abr. de 2015.

CARNEIRO, Adeneele Garcia - **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação** - In: Âmbito Jurídico, Rio Grande, XV, n. 99, abr 2012. Disponível em: <http://www.ambito-juridico.com.br/site/index.php/?n_link=revista_artigos_leitura&artigo_id=11529&revista_caderno=17>. Acesso em 19 nov 2014.

CENTRAL NACIONAL DE DENÚNCIAS AOS CRIMES CIBERNÉTICOS - Disponível em: <http://www.safernet.org.br/site/institucional/projetos/cnd>; Acesso em: 19 nov. 2014.

CENTRO DE TECNOLOGIA E SOCIEDADE – Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas - **Comentários e Sugestões sobre o Projeto de Lei de Crimes Eletrônicos (PL n. 84/99) -** In Biblioteca Digital da Fundação Getúlio Vargas, Rio de Janeiro, Ago 2008. Acesso em 19 nov. 2014

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

ERDELY, Maria Fernanda - **Itamaraty ainda estuda adesão à Convenção de Budapeste** - Disponível em: < http://www.conjur.com.br/2008-mai-29/itamaraty_ainda_estuda_adesao convencao_budapeste >. Acesso em: 03 de abr. de 2015.

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

GÓIS, Fábio - **O que dizem os dois projetos sobre "cibercrimes" -** Congresso em Foco. Disponível em: < http://congressoemfoco.uol.com.br/noticias/reportagens-especiais/o-que-dizem-os-dois-principais-projetos-sobre-%E2%80%9Ccibercrimes%E2%80%9D/> . Acesso em: 01 de abr. de 2015.

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-aceleratramitacao-de-projeto-de-lei-sobre-crimes-ciberneticos>.
Acesso em: 19 de nov. 2014

MONTEIRO, César Macedo. **Crime Virtual: Os paradigmas apresentados a luz da lei 12.737/2012.** Disponível em: <http://pt.slideshare.net/cmacedomonteiro/classificao-dos-crimes-de-informatica-ainda-sem-nota-de-rodap>Ano de 2014. Acesso em: 18 de nov. de 2014.

OLIVEIRA, Jôline Cristina de - **O Cibercrime e as Leis 12.735 e 12.737/2012** - Conteúdo Jurídico, Brasília-DF: 11 out. 2013. Disponível em: <http://www.conteudojuridico.com.br/?artigos&ver=1055.45489&seo=1>. Acesso em: 19 nov. 2014.

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

SILVA, Ana Karolina Calado da - **O estudo comparado dos crimes cibernéticos: uma abordagem instrumentalista-constitucional acerca da sua produção probatória em contraponto à jurisprudência contemporânea brasileira -** Âmbito Jurídico. 2012 Disponível em: <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=12778>; Acesso em: 11 de abr. de 2015.

SOUZA, Gill Lopes Macedo de. PEREIRA, Dalliana Vilar - **A Convenção de Budapeste e as leis brasileiras -** Disponível em: <http://charlieoscartango.com.br/Images/A%20convencao%20de%20Budapeste%20e%20as%20leis%20brasileiras.pdf>; Acesso em: 03 de abr. de 2015.

VALENÇA, Elisângela - **Sergipe já criou delegacia especializada em crimes cibernéticos -** F5 News. Disponível em: < http://www.f5news.com.br/10661_sergipe-ja-criou-delegacia-especializada-em-crimes-ciberneticos.html>; Acesso em: 18 de abr. de 2015.

CYBERCRIME: Challenges and prospects for the Brazilian Legislation

ABSTRACT

This study aims to discuss about the Law 12.737 / 2012 (popularly known as " Carolina Dieckmann Law"), which added legal provisions to criminalize cybercrime. Starting from the premise that the creation of the law filled a gap in the brazilian legislation on the subject, it is clear that there has been considerable progress in security question in the virtual world in our legal system. And that way, the objective is to understand the whole process of

developing devices in combat Cybercrime. Starts on bills with comparative analysis and legislation of other countries, as well as case law and doctrinal vision, aiming to unravel its contents and bring the information society that is immersed in the virtual world. Finally, the study will draw on screen prospects brought about by the new law and the changes to users of the worldwide web.

Keywords: Cybercrime. Law 12.737 / 2012. Carolina Dieckmann Law.

---

[1] Graduanda em Direito pela Universidade Tiradentes – UNIT. E-mail: vieira_camiila@hotmail.com