REVISTA TRANSGRESSÕES
Ciências Criminais em Debate

CRIMES CIBERNÉTICOS: GENERALIDADES E PERSPECTIVA DA LEGISLAÇÃO BRASILEIRA

Cícero Alves de Sousa Neto*
Matheus Santos**

RESUMO

O artigo fundamentar-se-á em uma breve abordagem indutiva introdutória sobre o conceito de crime cibernético, classificação, e outros termos essenciais, seguida pela nominação dos principais crimes cibernéticos cometidos atualmente. O estudo será contemplado com a exposição dos processos de denúncia e de acusação adotados para solucionar esse tipo de crime. Dando procedência a questão processual, será abordado o exercício de defesa, apontando o campo de atuação do criminoso, a origem e motivação do delito, incluindo para a esfera dos menores infratores. Será explanado como a legislação Brasileira lida com esse novo tipo de crime, em conjunto com uma abordagem crítica para a eficácia e eficiência das nossas normas legais. Complementando, se fará uma dialética das leis brasileiras com as normas legais de outros países. O intuito do Direito comparado é o de constatar a atualização e o nível de preparação do conjunto de leis para lidar com tal crime.

Palavras-chave: Crime cibernético. Generalidades. Aspectos Processuais. Legislação Brasileira. Direito Comparado

1 INTRODUÇÃO

Na contemporaneidade, a sociedade mundial vive uma, cada vez mais intensa, globalização, sustentada pela revolução tecnológica. Esse fenômeno conjunto ocasionou uma verdadeira dependência das pessoas por informação, computadores, celulares, entre outros.

Dentre os inúmeros aparelhos tecnológicos importantes na nossa vida, o computador é definitivamente o mais relevante, o qual consiste uma máquina processadora de dados, que possibilita operações importantes do nosso dia-a-dia em pouco tempo, como o armazenamento de uma vasta quantidade de dados.

O primeiro computador foi criado em 1946, e a *internet*, em 1969, ambas criações do governo americano no intuito de experiências militares. A *internet* chegou ao Brasil em 1988,

* Graduando do curso de Direito do Centro Universitário do Rio Grande do Norte, UNI-RN.
** Graduando do curso de Direito do Centro Universitário do Rio Grande do Norte, UNI-RN.

sendo comercialmente explorada em 1994. É óbvia a sua influência no fenômeno jurídico desde a sua criação, principalmente na investigação, e na agilização processual.

2 CONCEITO, CLASSIFICAÇÃO E TIPIFICAÇÃO DE CRIMES CIBERNÉTICOS

A sociedade mundial, desde a Idade Moderna, vivencia sucessivas revoluções. A mais recente desses fenômenos revolucionários foi a de caráter tecnológico, iniciado e aperfeiçoado pela indústria bélica e industrial no decorrer das grandes guerras mundiais, e tornando-se independente desde a metade do século XX. Dentro dessa revolução tecnológica, percebemos uma série de inovações, alastrando mais ainda tal fenômeno, abrangendo inclusive para o uso dessas novidades com intuito cometer crimes ou tirar vantagens.

O crime cibernético não envolve apenas a *internet*, mas o sistema informático por completo, os crimes praticados via *internet* são apenas uma área, um ramo.

O crime cibernético é aquele que é praticado contra o sistema informático ou através dele, compreendendo os crimes praticados contra o computador e seus acessórios ou através deste. Inclui-se neste conceito os delitos praticados através da *internet* (CASTRO, 2001, p. 10).

2.1 Crime Próprio e Impróprio

Na nossa legislação, algumas condutas desse tipo de crime são definidas e amparadas por lei, mas sem eficiência e eficácia, perpetuando a impunidade, e até mais que isso, a cifra negra.

Os crimes de informática próprios são aqueles unicamente provocados através da informática, com o alvo inserido em seu sistema, por exemplo: pichação de *homepages*, envio de vírus, vandalismo na rede, pirataria de *software*, violação de *e-mail*, entre outros.

Os crimes cibernéticos impróprios, o agente utiliza a informática como canal, mas seu alvo está fora dela, fora do sistema, por exemplo: ameaça, estelionato, calúnia, pedofilia, entre outros.

2.2 Sujeito Ativo e Passivo

O sujeito ativo da conduta delituosa é aquele que utiliza de seus conhecimentos informáticos para o cometimento do crime, visando o benefício próprio e/ou prejuízo de terceiros. Por outro lado, o sujeito passivo é o tutelar de bem jurídico lesado por outrem (sujeito ativo). Nos crimes cibernéticos, são todos aqueles que são lesados pela utilização de métodos ou meios informáticos.

Qualquer indivíduo pode ser sujeito ativo nos crimes cibernéticos, muitos são, e não tem consciência disso, devido à falta de informação.

A maioria dos crimes cibernéticos é cometida por ex-funcionários de empresas do ramo tecnológico, contra a mesma, em razão de um descaso ou insatisfação, associado a uma habilidade adquirida com a experiência. Além de terem acesso a senhas, conhecem funcionários, servidores, parceiros, e clientes. (CASTRO, 2001, p. 13).

Qualquer um pode ser sujeito passivo, mas, como foi exposto, logicamente, as vítimas mais constantes são empresas relacionadas com a área tecnológica. O problema é que, a maioria dessas empresas prefere não realizar a denúncia, e arcar com os prejuízos. A vitimologia mostra que a razão principal dessa atitude está na não confiança do trabalho dos órgãos de segurança pública, tanto por parte de pessoas físicas como jurídicas.

2.3 Lugar do Crime

Alguns casos de crimes cibernéticos ocorrem em escala internacional, por isso que a determinação do lugar é imprescindível para aplicação ou não da lei brasileira.

A seguir, nos deparamos com exemplos de casos em que a legislação do Brasil age para controlá-los: A (na Inglaterra) envia *e-mail* contendo vírus para B (no Brasil); A (no Brasil), envia *e-mail* com ameaça para B (fora); A (fora), envia fotos de pornografia infantil para B (fora), que as envia para C (no Brasil), que as publica; e por fim, A (fora), envia *e-mail* para B(fora), porém C (no Brasil), intercepta (CASTRO, 2001, p. 15).

2.4 Crimes Contra a Honra

Segundo os artigos 138, 139 e 140 do Código Penal (CP) Brasileiro, os crimes contra a honra podem ser de três tipos: calúnia (art.138), difamação (art.139), e injúria (art.140). Para consistir em crime de calúnia ou difamação, é obrigatório a existência de uma terceira pessoa, se ninguém, além do ofendido, não testemunhar a ofensa, o crime não existe. Na injúria, a

vítima não é imutada de um fato material, mas sim de uma característica. Em caso do crime ser de imprensa, o processo cai sobre a pessoa jurídica.

A maioria dos Magistrados utiliza o próprio CP para caracterizar crimes comuns praticados na internet, os crimes contra a honra são alguns deles. A diferença do crime contra a honra comum para o virtual são os meios utilizados na prática desta conduta delituosa.

O CP estipula como pena do crime de calúnia um período de 6 meses a 2 anos (detenção); crime de difamação, a detenção dura de 3 meses a 1 ano; e para a injúria, o indivíduo pode ser detido de 1 a 6 meses; todos acrescidos de multa. Vale salientar que os crimes contra a honra de caráter cibernético são considerados como impróprios.

2.5 Interceptação de E-mail

O sigilo de correspondências é garantido pelo inciso 12 do artigo 5º da Constituição Federal (CF), e o *e-mail* está incluído no rol exposto na Carta Magna. Interceptar é impedir. Percebe-se uma antinomia no texto do CP (trata tal crime com generalidade no art.180), e norma legal esparsa nº 9.296\96 (tratando o *e-mail* de forma específica, por ser uma comunicação feita pela *internet*, consequentemente, especificando melhor o crime). O crime de interceptação de *e-mail* é classificado como próprio, e é válido para pessoa física ou jurídica. A pena de reclusão pode durar de 2 a 4 anos.

Geralmente esse tipo de crime ocorre quando o agente ativo, motivado a obter alguma vantagem ou com o *animus nocendi*, utiliza dos meios informáticos para obter informações contidas no endereço eletrônico de outrem. Podemos perceber que a obtenção ilícita de senha, para monitoramento do endereço eletrônico, constitui também esse tipo penal.

2.6 Revelação de Segredo

Conforme está previsto nos art. 153 e 154 do CP, o crime de revelação de segredo consiste na divulgação, sem justa causa, ou permissão, de qualquer informação que provoque danos morais ou econômicos a outrem (podendo ser pessoa física ou jurídica). É *mister* ressaltar que o indivíduo pode praticar tal delito sem utilizar de instrumentos tecnológicos.

Referente aos crimes contra a administração Pública, se as informações não forem, por lei, considerada sigilosas, não ocorre crime. Porém, caso o delito seja constatado, a penalidade é mais grave do que se a vítima for um particular.

No que remete as questões cibernéticas, o sistema de informática é apenas o canal, o caminho para o fim, que não encontra-se nele. Resta, durante a investigação, descobrir qual era a intenção do delinquente, ao revelar o segredo de alguém.

Por fim, classifica-se o crime de revelação de segredo como impróprio e sua pena varia bastante: caso seja a vítima uma pessoa física, 1 a 6 meses de detenção e multa; se a vítima for a administração pública, 1 a 4 anos de detenção e multa. É importante lembrar que o parágrafo 2º do art. 154-A estipula o acréscimo de um terço a um sexto, caso seja provado algum dano econômico.

Em Junho deste ano, o caso do americano Edward Joseph Snowden, que delatou os procedimentos da inteligência e Segurança Americana, obteve uma grande repercussão internacional. Além da interferência na soberania de vários países, Snowden conta que o Governo Americano espionava seus cidadãos, monitorando vários dos grandes provedores de informação digital.

2.7 Ciberterrorismo

Ciberterrorismo é a designação para a prática do terrorismo utilizando os meios computacionais, o que amplia o fenômeno terrorista. Em 2010, um caso de grande repercussão internacional foi a utilização de um "Vírus", denominado Stuxnet, com intuito de invadir usinas nucleares, como as do Irã e na Índia. Práticas como esta podem resultar em grandes catástrofes, mostrando o real potencial ofensivo desta modalidade de terrorismo.

O ciberterrorismo pode englobar pelo menos três fenômenos: ataques realizados através da rede de computadores, a disseminação de conteúdo ilegal nos sistemas de computação, ou o uso da internet para servir de meio de comunicação (RBCCrim,2012).

Em novembro de 2011, foi criada a Convenção sobre o Crime Cibernético do Conselho da Europa, ratificada por mais de 30 Estados nacionais, os quais introduziram em seus ordenamentos jurídicos, alguns importantes instrumentos de combate ao ciberterrorismo. Foi a partir dessa convenção que se criminalizou algumas condutas como: acesso ilícito e ataque a sistema de informática; fraude informática; atos xenofóbicos; e outras mais sobre a responsabilidade penal do infrator.

Na atualidade existem elementos notórios no que diz respeito a prevenção e controle do ciberterrorismo, como o papel dos provedores e serviços de internet na investigação. Além disso, nota-se o grande dilema entre a preservação dos direitos fundamentais e as ações de

investigação para identificar os crimes cibernéticos, que devem alcançar o nível mais específico possível. Essa antinomia deve ser tratada com cautela e equidade.

2.8 Pedofilia

Pedofilia é uma conduta sexual caracterizada pela atração sexual por crianças, sem distinção de gênero. Diferentemente do que muitas pessoas imaginam, o pedófilo difere, e muito, daquele que molesta sexualmente crianças. Atos isolados e individuais não podem ser caracterizados como pedofilia.

A partir do momento em que as pessoas passaram a ter o acesso à *internet*, já inseriram a pornografia para uso comum. No aproveitamento, muitos indivíduos tomaram proveito para divulgar fotos de conteúdo obsceno relacionado à pedofilia, que, dentre toda a gama dos crimes cibernéticos, é o mais repudiado socialmente, em razão do constrangimento provocado na criança, que a afeta para toda a vida, e podendo desencadear vários transtornos psicológicos.

O indivíduo que constatar tal crime deve denunciá-lo, apontando o *site* vinculador. Os criminosos tem o perfil de obsessão por crianças, são geralmente casados e insatisfeitos sexualmente. O Estatuto da Criança e do Adolescente define criança o indivíduo até 12 anos. Vale acentuar que o crime consuma-se tanto no ato do armazenamento, como no de publicação, conforme está vinculado no art. 241-A, do estatuto. Ausente conhecimento da parte do imputado, não há dolo, pois existem casos de indivíduos que vinculam acreditando que as vítimas são maiores de idade.

Esse tipo de conteúdo é muito fácil de ser acessado. Servidores estrangeiros armazenam-no sem nenhuma restrição e sem fiscalização. A maior parte deste conteúdo encontra-se na chamada *Deep Web* ou *Darknet*.

O conteúdo varia entre fotos, vídeos, técnicas de sedução, de coação, entre outros. Em nossa legislação é considerado conteúdo pedófilo, qualquer imagem ou vídeo contendo imagens de impúberes praticando relações sexuais ou qualquer imagem que erotize a imagem da criança.

3 IMPUTAÇÃO

A imputação consiste na narrativa dos fatos, em tese criminal, feita pelo Ministério Público. Esse documento deve ser extremamente detalhado, visto que não basta acusar o réu somente com base nos fatos, é necessário da parte do MP apontar a sua conduta enquanto criminoso. Nos crimes cibernéticos, os detalhes consistem de muita relevância no processo penal.

O julgamento deve ser *citra petita*, ou seja, o magistrado deixa de analisar algo que tenha sido pretendido pela parte ou tenha sido trazido como fundamento do seu pedido ou da sua defesa. A acusação deve acentuar todos os meios pelos quais o criminoso utilizou para delinquir.

3.1 Prova Mínima

Deve-se ter um suporte mínimo para dar início a uma ação penal. Destarte, o MP procura apontar de maneira precisa e objetiva a existência do crime, identificando a máquina utilizada. Porém, a dificuldade é visualizada quando o computador utilizado encontra-se em locais públicos (Universidades, lan houses, lojas). Apenas a denúncia não ajudará na resolução, e a identificação do autor ficará comprometida. É *mister* ressaltar que é incabível acusar o proprietário.

Confirma que é simplesmente uma prova necessária e cabível para condenar alguém (testemunha, *e-mail*).

Se a denúncia não oferecer suporte, não deve ser aceita, mas caso seja, a defesa poderá impetrar o *habeas corpus*.

3.2 Queixa do Crime e Assistência Acusatória – Possibilidade

A ação penal pode ser privada (denúncia particular) ou pública (denúncia do MP, que é o mais comum). Porém existe uma série de tipos de delitos como os crimes contra a honra, ou envio de vírus, que devem obviamente iniciar por denúncia privada, já que somente o particular poderá constatar o crime, nesses casos, o Magistrado volve a queixa para o MP, que poderá optar por recebê-la, e construir uma denúncia substitutiva.

Se ação penal for pública, ou seja, tutelada pelo MP, o ofendido ou seu representante podem auxiliar o MP. Em caso de morte da vítima, conforme se encontra no art.12 do Código Civil, ela pode ser curatelada pelo cônjuge, ascendente, descendente.

O assistente só ingressa na causa oficialmente após a denúncia, podendo ele recolher provas, requerer testemunhas, e pedir recursos.

4 DA DEFESA

A dificuldade investigatória não está na identificação da máquina operante, mas do delinquente, pois na grande maioria dos casos, como já foi exposto, o computador utilizado para delinquir é usado por várias pessoas, daí a necessidade de uma prova mínima extremamente fundamentada. Esse fato pode consistir no trancamento da ação penal por parte do advogado de defesa, devido à falta de Legislação ou até mesmo Justa Causa.

A paralisação da ação penal, feita pelo advogado de defesa, é realizada, como já se sabe, a partir da impetração de *habeas corpus*, posto que o Juiz já acatou a denúncia. Outro caso que ocasiona chances de trancamento da ação é se o MP imputar o réu de um fato não previsto em lei. Devido a ineficácia de algumas normas legais, é comum a sustentação de comportamento atípico, mas não criminoso (ou seja, que não está legalmente definido), é o caso do crime de envio de vírus, caso esse programa estranho ao computador não provoque prejuízos financeiros.

Especificamente os crimes de pedofilia expõem casos que dificultam a imputação de indivíduos. É o caso de pessoas que divulgaram a foto de menores, porém, as vítimas apresentam certa culpabilidade, pois afirmaram que já possuíam a maioridade. Tal ocasião é favorecida quando a fisionomia da vítima aparenta que ela é realmente mais velha e consequentemente maior de idade. Nessas ocasiões, não existe dolo, tornando a tarefa do Promotor de acusá-lo quase impossível, e a causa passa a caminhar para a absolvição.

Outro exemplo, ainda envolvendo o crime de pedofilia, é de um indivíduo que publica as fotos de um menor, sem ter o conhecido, ainda mais quando sua fisionomia da vítima é aparentemente adulta (adolescentes de 16 e 17 anos principalmente). Nessa ocasião, não há possibilidade de imputação, a não ser que seja explícita a jovialidade da vítima (no caso da vítima ser uma criança de 7 anos, por exemplo).

4.1 Do Menor Infrator

O Estatuto da Criança e do Adolescente dispõe da proteção integral da parte do Estado para com crianças (0 a 12 anos incompletos) e adolescentes (12 a 18 anos incompletos), caracterizando-os como indivíduos inimputáveis. Percebe-se a diferença de tratamento do Estado, que considera o menor como apreendido, que cometeu atos infracionais, e que passará por medidas socioeducativas.

O menor infrator deve passar por um acompanhamento que não faça com que ele venha a delinquir novamente, para não permanecer na vida criminosa (CASTRO, 2001, p. 113). Esse acompanhamento é a medida socioeducativa, que compreende uma advertência, ou a obrigação de reparar o dano causado, ou a internação, ou a liberdade assistida, além da orientação, assim como o encaminhamento aos pais ou responsáveis, e por fim, a inclusão em tratamento comunitário, alcoólico, tóxico, entre outros.

O número de infrações penais cometidos por menores de idade só aumenta, inclusive de caráter cibernético, visto que é comum menores, que estão em seu desenvolvimento sexual, acessarem *sites* pornográficos, e neles, procurem imagens ou vídeos de pessoas de mesma faixa etária. Pode ser que ao armazenar\vincular fotos de menores (crime de pedofilia), o menor não tenha a intenção de cometê-lo. Fato é que fatores subjetivos são importantíssimos a ponto de mudar totalmente a ação penal. Para tal, a personalidade do menor deve ser avaliada, assim como a circunstância. Em casos similares, o magistrado deve aplicar as medidas socioeducativas, exceto em crimes contra o patrimônio, os quais o Juiz geralmente emite a reparação do dano.

5 CENÁRIO LEGISLATIVO BRASILEIRO ATUAL

Após a incidência no que diz respeito as esferas doutrinária e processual, é *mister* trazer à baila a matéria do direito material. Deve-se estar em observância com a legislação por razão óbvia, para que se possa obter ciência, de quando um direito do cidadão foi violado ou ameaçado.

Partindo para uma esfera de análise, poderemos perceber como a legislação brasileira está se portando perante os crimes cibernéticos, como define-os, como a pena é individualizada nos preceitos secundários, e por fim, qual o grau de relevância dado ao legislador brasileiro para esse produto negativo das novas relações sociais.

5.1 Lei nº 12.737\12 (Lei "Carolina Dieckmann")

Sancionada no mês de dezembro do ano de 2012, a lei ficou conhecida com o nome da atriz Carolina Dieckmann. Obteve esse nome devido a atriz ter seu computador invadido por *crackers*, e logo em seguida, ter sido divulgado na internet algumas imagens pessoais da dela. Além do crime de interceptação de e-mail, houve o crime de extorsão, pois os *crackers* exigiram da atriz uma pecúnia de R$10.000,00 para que as imagens não fossem divulgadas.

A Lei entrou em vigor dia 3 de abril de 2012, e no ano seguinte, incorporada ao art. 154 do CP, estabelece a pena para a invasão de dispositivo alheio, sem motivo ou sem consentimento do dono, de 3 meses a um 1 ano, sob possibilidade de aumento, caso provoque prejuízos econômicos a vítima, ou se a vítima for a administração pública (membros do executivo, presidentes do Supremo Tribunal Federal, Câmara dos Deputados, Câmara do Senado, entre outros). Além da detenção, a pena de multa também está prefixada.

5.2 A Pioneira Lei nº 9.609\98 (Lei para Proteção de Propriedade Intelectual e Programas de Computador)

Essa norma legal considera o programa de computador um importante organizador de informações necessárias. Sobre o direito autoral, define como sendo o direito patrimonial e moral do autor da sua obra intelectual, científica, ou artística. Por isso, a lei nº 9.609\98 assegura a reivindicação e tutela por parte dos criadores/donos do programa, e autores da obra violados.

O crime em questão possui uma ação múltipla. No caso dos programas, pode-se constatar a reprodução não autorizada, a alteração, o acréscimo ou a retirada de informações, e tratando-se dos direitos autorais, pode ser a reprodução não autorizada (muito mais comum), a venda, a exposição, ou a troca (CASTRO, 2001, p. 32).

A lei nº 9.609\98 determina a penalidade de 6 meses a 2 anos ou multa, para o invasor de programas de computador, e o violador de direito autorais. Vale salientar que a sanção pode ser mais grave (1 a 4 anos), caso exista a reprodução indevida do programa, ou obra.

5.3 Perspectiva Crítica da Legislação Brasileira

O Brasil precisa urgentemente criar uma legislação específica para crimes cibernéticos, uma vez que a internet hoje se tornou indispensável para a sociedade, através de um caráter de informação, trabalho e lazer.

Após a realização deste estudo, se faz necessário a imediata tipificação em nosso ordenamento jurídico de condutas criminosas praticadas por meio da internet. O Brasil está atrasado no aspecto jurídico, devendo-se igualar aos países que já possuem legislação específica para crimes virtuais, para que não sejamos um paraíso aos criminosos desse setor.

A jurisprudência nacional tem se mostrado a favor da responsabilização/condenação dos indivíduos que cometem delitos por meio da internet, mas por haver lacunas no ordenamento jurídico, ainda existem criminosos que não podem ser condenados.

6 DIREITO COMPARADO

Um estudo de Direito Comparado permite-nos observar o tratamento dado por outros países a um determinado instituto jurídico em comum com a nossa legislação. Muitas vezes, os axiomas e valores sociais substancias diferenciados entre países pode não fornecer uma análise precisa do objeto de estudo. Mas, no caso dos crimes cibernéticos, o estudo de Direito Comparado faz-se necessário, em razão dos crimes digitais serem produtos de uma revolução de escala mundial, que por conseguinte, torna-o presente em todas as estruturas sociais.

Por essa razão, outra constatação emerge, a de que o *Inter Criminis* do agente é bastante similar em qualquer local que ele cometa a infração penal, o que nos permite concluir que, absolvendo os métodos de como outros países lidam com os crimes cibernéticos, podemos obter uma matéria substancial para que a legislação brasileira saiba amparar de uma forma mais taxativa esse tipo de conduta.

6.1 Direito Alemão

Destarte, a corte constitucional Alemã, ao tratar da legislação que define os crimes virtuais, estabeleceu o respeito aos direitos fundamentais prefixados no art. 1º, § 1º, da constituição Alemã. Optando pela primeira alternativa sugerida pela própria corte, relativa ao monitoramento da internet, ressaltando o acesso secreto apenas para casos importantes (segurança nacional, bem público, entre outros).

Porém, após a decisão, a corte Alemã se deparou com o caso dos provedores de comunicação eletrônica, os quais, por mais que sejam parte privadas, prestavam também, serviços públicos. Esses provedores atuavam armazenando informações confidenciais dos indivíduos por um período de 6 meses, agindo de acordo com o art. 10 da lei de reforma do setor de comunicações (GG). Depara-se novamente a corte Alemã, com o dilema do abuso de autoridade, e a preservação da segurança nacional.

Por fim, a corte constitucional Alemã muda seu parecer sobre a legislação definidora dos crimes cibernéticos, e decide por um requisito prévio de legitimação para colheita de dados em um período de 6 meses, no intuito de traçar um perfil dos usuários, buscando a integridade da segurança nacional. O resultado é que quando um determinado indivíduo for pelo menos suspeito de imputação, o órgão investigativo já esteja norteado e ciente das características do provável criminoso (RBCCrim,2012).

6.2 Direito Sueco

Devido ao seu pioneirismo quanto ao amparo do seu ordenamento jurídico aos crimes cibernéticos, a Suécia merece destaque. Seu CPP entrou em vigência no ano de 1948, e percebe-se uma espécie de democracia experimental, aplicada tanto na área cível, como na área penal, visto que quem conduz o processo, não é o magistrado, são as partes, e o autor, é o promotor de justiça (RBCCrim,2012).

Algumas provas já são colhidas por investigação preliminar da polícia, surgindo uma ação penal/cível, investiga-se de maneira mais visceral. É importante lembrar que não existem normas legais vigentes que determinem a apreciação das provas, ou exclusão delas dos processos.

6.3 Direito Norte-Americano

Os Estados Unidos possuem um regime jurídico misto, por um lado legalista (constituição federalista), mas por outro, um sistema baseado nos precedentes jurídicos e no costume jurídico, também conhecido como *Common Law*, a partir disso, pode-se inferir que os Estados Unidos possuem um sistema jurídico muito complexo.

O início da prevenção aos crimes cibernéticos ocorreu na década de 80, quando o pós-graduando Robert Tappan Morris realizou um experimento para descobrir falhas em

sistemas informáticos, através de um vírus que se auto reproduzia para outros sistemas, ocasionando um resultado maior do que ele mesmo esperava.

A codificação é claramente majoritária em relação aos ilícitos decorrentes de decisões judiciais no Direito Penal Norte Americano. A legislação é extremamente específica, tanto em escala federal, como estadual. Em 1981 surgiu a Lei de proteção aos sistemas computacionais (*Federal Computer System Protection Act*), a qual criminaliza a fraude, furto ou qualquer tipo de apropriação indébita de sistemas computacionais. No ano seguinte, em 1982, surge a lei de transferência de fundos eletrônicos (*Eletronic Funds Transfer Act*), a qual regulamenta a transferência e vinculação das fraudes de um determinado sistema.

Porém, a principal norma legal de prevenção aos crimes cibernéticos, nos Estados Unidos, foi publicada em 1986: a chamada Lei de Fraude e Abuso Computacional (*Computer Fraud and Act*). Essa norma legal pretende proteger a acessibilidade ao sistema computacional, visando obter vantagens financeiras.

7 CONCLUSÃO

Após estudo sobre o tema, pode se constatar um aprimoramento do que seria um crime cibernético, não se tratando simplesmente de uma invasão indevida ao disposto informático alheio, como consta no *caput* do art.154-A do Código Penal, mas sim um crime com uma finalidade de agir bem peculiar, tratando-se da obtenção, adulteração ou destruição de informações ou dados sem autorização do titular do dispositivo.

Nesse momento, se pode ter uma melhor noção do compromisso que a sociedade brasileira deve ter ao tratar dos crimes cibernéticos, pois estes encontram-se mais presentes no nosso dia-dia do que podemos imaginar. É por essa razão, que se deve estimular os representantes do povo a estudarem as legislações internacionais específicas do tema, e adequá-las com a realidade social do Brasil, pois o nosso país ainda é muito carente quando volve-se para uma conduta ilícita tão recente.

REFERÊNCIAS

CASTRO, Carla Rodrigues Araújo de. ***Crimes de Informática e seus aspectos processuais*.** Rio de Janeiro: Lumen Juris, 2001.

CORRÊA, Gustavo. ***Aspectos Jurídicos na internet*.** 3. ed. São Paulo: Saraiva, 2007.

DIDIER JR., Fredie. ***Curso de Direito Processual Civil***. 15. ed. Salvador: Jus Podivm, 2013. v. II.

PINHEIRO, Patrícia Peck. ***Direito Digital*.** 4 ed. São Paulo: Saraiva, 2010.

VIEIRA, Jair Lot. ***Crimes na internet: interpretados pelos tribunais: repertório de jurisprudência e legislação*.** Bauru: Edipro, 2009.

SILVA, Ana Karolina da. **O estudo comparado dos crimes cibernéticos:** uma abordagem instrumentalista-constitucional acerca da sua produção probatória em contraponto à jurisprudência contemporânea brasileira. **Âmbito Jurídico**, Rio Grande, fev. 2013. Disponível em: <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=12778>. Acesso em: 18 ago. 2013.

CYBERCRIMES: GENERAL AND BRAZILIAN LAW PERSPECTIVE

ABSTRACT

The article will be based on a brief introductory inductive approach on the concept of cybercrime, rating, and other essential terms, followed by the nomination of the major cybercrimes currently committed. The study will be awarded exposure of procedures for complaint and accusation adopted to solve this crime. Giving precedence to procedural issue, we will address the defense exercise, pointing the playing field of the criminal, the origin and motivation of the crime, including to the sphere of juvenile offenders. Will be explained as the Brazilian legislation deals with this new type of crime, together with a critical approach to the effectiveness and efficiency of our legal standards. Complementing will be a dialectic of Brazilian law with the laws of other countries. The purpose of comparative law is to note the update and the preparedness of the set of laws to deal with such crime.

Keywords: Cybercrime. General. Procedural aspects. Brazilian law. Comparative law.