

A PROBLEMÁTICA DA AUSÊNCIA LEGISLATIVA EM RELAÇÃO AOS CRIMES VIRTUAIS

Aluno: Amanda da Silva Cazetta*

Orientador: Galvão Rabelo**

SUMÁRIO: Introdução. 1. Conceito e características dos crimes virtuais. 2. Principais crimes virtuais praticados na atualidade. 3. Ausência de legislação específica e repressão dos crimes informáticos. 4. As principais propostas legislativas sobre os crimes virtuais. Conclusão. Referências Bibliográficas.

RESUMO

A sociedade e o mundo passaram por diversas modificações, e com elas o Direito também deve ser alterado, inclusive o Direito Penal, mesmo sendo considerado a última alternativa a ser utilizada. Faz-se necessário criar novas leis para tipificar os crimes virtuais, que além de afetar bens jurídicos já protegidos, estabelecem novos a serem acobertados pela lei. Os crimes virtuais estão atingindo cada vez mais a população, por falta de punição à sua prática. No Brasil ainda não existe uma legislação específica para aplicar as penas devidas a fim de repreender estes crimes, apesar de já existirem vários projetos de lei, que há anos circulam pelo Poder Legislativo. A ausência de lei sobre o tema esbarra no princípio da legalidade e na proibição da analogia “in malam partem”, o que constitui incentivo para que os legisladores impulsionem estas novas leis, a fim de que o Estado tenha respaldo legal para punir estes criminosos.

PALAVRAS-CHAVE: Crimes virtuais. Legislação específica. Princípio da legalidade penal. Proibição da analogia *in malam partem*.

* Acadêmica do 10º período do Curso de Direito da Faculdade Presidente Antônio Carlos (FUPAC) - Ubá; E-mail: aman_sc@hotmail.com.

** Professor graduado em Direito pela Universidade Federal de Viçosa. Especialista em Ciências Penais pela Universidade Federal de Juiz de Fora. Advogado.

INTRODUÇÃO

Nos dias atuais, não é possível visualizar nossas vidas sem os meios de comunicação. São eles que fazem a ligação entre os povos, além de outros inúmeros benefícios que trazem a todos. Um dos mais importantes meios de comunicação é a internet, através da qual se abre um mundo de possibilidades para as pessoas. No entanto, ela também pode ser usada de forma negativa, com o objetivo de cometer os mais variados tipos penais.

Criada em meados de 1960 aproximadamente, no auge da Guerra Fria, a internet, tomou uma dimensão que em seus primeiros anos nunca foi imaginada. Ela trouxe à sociedade uma evolução que aconteceu de forma muito rápida. Mas, assim como a sociedade foi beneficiada com essas inúmeras inovações, o crime também se adaptou a essa nova tecnologia, passando a existir uma nova preocupação: a prática de delitos no “ciberespaço”.

A sociedade tem sofrido com a falta de punição a estes crimes que se utilizam do computador e da internet, porque o nosso ordenamento jurídico não acompanhou a evolução deste meio de comunicação, com a consequente elaboração de leis específicas para estes delitos.

A falta de legislação específica para a coerção destas condutas tem sido tema muito discutido no meio jurídico, assim como a dificuldade que o Estado tem de impor sanções a esses criminosos, pois o Direito ainda não acompanhou, neste aspecto, as mudanças sociais trazidas pela informática.

Diante da mencionada ausência de legislação penal especificamente voltada para a tipificação das condutas que caracterizam os chamados “crimes informáticos”, e considerando sua notória lesividade social, é de se questionar: como as instâncias penais têm atuado na repressão desses crimes? A existência de uma legislação específica para essa modalidade de crimes ajudaria em sua repressão?

O objetivo do presente artigo é compreender, a partir de uma visualização bem ampla (e, por isso mesmo, não exauriente), a dinâmica dos

crimes virtuais na sociedade contemporânea e como a ausência de legislação penal especificamente voltada para o tema pode concorrer para a impunidade de tais condutas.

A pesquisa se justifica, uma vez que tais práticas são frequentemente praticadas no cotidiano de nosso país e, por se tratar de um novo problema social, está a demandar estudos para uma melhor compreensão da questão e para a adoção de formas juridicamente adequadas para enfrentá-lo.

1. CONCEITO E CARACTERÍSTICAS DOS CRIMES VIRTUAIS

Antes de adentrar-se no tema – crimes virtuais –, é importante saber a origem do computador e da internet, visto que são as duas ferramentas essenciais deste tipo de crime.

Os primeiros computadores começaram a surgir no início da década de 1950¹. Eram logicamente muito menos evoluídos do que os atuais, mas já conseguiam fazer cálculos complexos em um rápido intervalo de tempo. Estes primeiros computadores ficaram conhecidos como computadores de 1ª geração. Posteriormente, surgiu a 2ª geração de computadores, que objetivavam reduzir os custos de manutenção com essas máquinas. Já a 3ª geração, utilizava-se de teclados e monitores que permitiam a visualização de certos sistemas operacionais. Mas, foi a partir da 4ª geração que se chega ao modelo utilizado atualmente, por causa dos microprocessadores que permitiram a redução das máquinas.

Mas, além dos computadores, é preciso outra ferramenta para se praticar delitos virtuais, qual seja, a internet, que é um mecanismo de disseminação de informação e divulgação mundial, e meio de colaboração entre indivíduos.

A internet surge em meio a Guerra Fria, em meados de 1960², a partir de um projeto da *Advanced Research Projects Agency* (ARPA) que idealizou

¹ HAMANN, 2011.

² WIKIPEDIA, História da internet, 2012.

um sistema para descentralização de informações: a ARPANET. Assim como o computador, a internet também evoluiu ao longo do tempo, mas foi só nos anos 90 que a internet começou a se popularizar no mundo, começando a ser utilizada para fins comerciais e para fornecimento de diversos serviços a nível mundial.

Este avanço só foi possível a partir do desenvolvimento do *Word Wide Web* (www.) pelo engenheiro Tim Bernes-Lee, o que possibilitou a criação de sites mais dinâmicos e mais chamativos visualmente.³ Aqui no Brasil, o sistema só era usado no meio acadêmico até o ano de 1995, depois disso se tornou público.

Com a abertura desta porta tecnológica foi possível aos criminosos ampliar seu espaço para a prática dos crimes. Acredita-se que na década de 60 já se iniciou a prática desses delitos que se resumiam em sabotagem, manipulação, espionagem e o uso abusivo dos computadores. Nos anos 80, a criminalidade nesse setor foi aumentando passando a áreas como pornografia infantil, pirataria, etc.

Passada a importante fase de explicação da evolução histórica dos meios fundamentais de execução dos crimes virtuais, computador e internet, faz-se necessário ingressar no conceito dessa modalidade de crimes.

São muitas as definições que procuram apreender essa modalidade de delitos e várias são as nomenclaturas utilizadas, como: crimes digitais, informáticos, cibernéticos, eletrônicos, e-crime, etc.⁴

Muitos doutrinadores têm elaborado um conceito para esses crimes em voga, como, por exemplo, Ivette Senise Ferreira que compreende como tal “toda ação típica, antijurídica e culpável, cometida contra ou pela utilização de processamento automático de dados ou sua transmissão”⁵, ou também definições trazidas por órgãos, como a Organização para Cooperação Econômica e Desenvolvimento da ONU que diz ser crime virtual “qualquer

³ SUA PESQUISA, história da internet.

⁴ WIKIPEDIA, Crime informático, 2012.

⁵ FERREIRA *apud* GUIMARÃES; FURNALETO NETO, 2003.

conduta ilegal, não ética, ou não autorizada que envolva o processamento automático de dados e/ou transmissão de dados”⁶.

Incorpora-se ainda a este artigo o conceito de crimes virtuais de Ramalho Terceiro:

[...] os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo, por isso, ficaram usualmente definidos como sendo crimes virtuais, ou seja, os delitos praticados por meio da internet são denominados de crimes virtuais, devido à ausência física de seus autores e seus asseclas.⁷

Segundo Augusto Rossini:

[...] o conceito de “delito informático” poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade.⁸

Retirando um pouco do entendimento de cada doutrinador, pode-se falar que *delitos virtuais são aquelas condutas danosas praticadas através do computador ou contra ele, que causam lesão a um bem jurídico protegido, sem a presença física do autor do delito no momento do fato.*

Alguns juristas chegam até a classificar penalmente os crimes virtuais, como Reginaldo César Pinheiro, que classificam estes crimes em puros, mistos e comuns. Seria *crime virtual puro* aquele que atenta contra a parte física e a virtual do microcomputador, ou seja, o hardware e software. O *delito virtual misto* tem objetivo diferente do anterior e neste, o criminoso se utiliza da internet para praticar a conduta ilícita. E por último, *crime virtual comum* é aquele que se utiliza da internet como ferramenta para cometer condutas típicas já constantes no Código Penal.⁹

Um último dado curioso sobre esses crimes é a nomenclatura vulgarmente utilizada para definir esse tipo de criminoso, *hacker*, no entanto devemos ficar atentos ao fato de que não se pode chamar assim todo

⁶ GUIMARÃES; FURNALETO NETO, 2003.

⁷ TERCEIRO *apud* PINHEIRO, 2006.

⁸ ROSSINI *apud* PINHEIRO, 2006.

⁹ PINHEIRO *apud* GUIMARÃES; FURNALETO NETO, 2003.

praticante desses crimes: tudo dependerá de qual destes crimes ele ira cometer.¹⁰

2. PRINCIPAIS CRIMES VIRTUAIS PRATICADOS NA ATUALIDADE

Atualmente a prática de crimes que se utilizam do computador e da internet é enorme e no Brasil ela vem crescendo cada vez mais. A multinacional em segurança na internet, Symantec, divulgou que no país, 54 pessoas por minuto são vítimas desses tipos de delito.¹¹

Como tais condutas danosas são muito variadas, serão abordadas neste trabalho apenas as principais dentre elas, e para ficar mais didático o estudo, será explicado de acordo com sua classificação.

Nos crimes virtuais considerados *impróprios*, o Estado tem até conseguido chegar a uma punição aos infratores, pois já existe uma tipificação destes, no Código Penal. São casos corriqueiros no dia a dia, os crimes de¹²:

- *Ameaça*: um tipo penal previsto no art. 147 do Código Penal, prevê que incide neste crime aquele que, por qualquer palavra, escrito ou gesto, anuncie mal injusto à vítima. Este mal deve ser injusto e grave e pode se configurar em e-mails com frases como “vou te pegar”, etc.
- *Participação em suicídio*: previsto no art. 122 do CP, este delito traz a ideia de que alguém ao ajudar, induzir ou instigar terceiro a se suicidar é criminalmente punível, quando a vítima de fato morre ou quando lhe sobrevém lesão corporal grave em decorrência do fato. E isso pode ocorrer, com criação de páginas em redes sociais que estimulem, através de comentários, que uma pessoa determinada tire a própria vida.
- *Crimes contra a honra*: estes se encontram nos arts. 138, 139 e 140 do CP e constituem um dos casos mais comuns na internet. A calúnia que

¹⁰ WIKIPEDIA, Crime informático, 2012.

¹¹ TECLAI, 2012.

¹² CRESPO, 2011, p. 72-75.

se caracteriza pela imputação falsa de crime a uma pessoa, é exemplificada quando alguém envia e-mails dizendo que um terceiro praticou determinado estupro. Já a difamação, ocorre quando é imputado fato ofensivo à reputação da vítima, como no caso em que se publica nas redes sociais que determinada pessoa está se drogando. Por último, a injúria constitui ofensa a honra subjetiva do indivíduo, e pode se dar da mesma forma que acontece nos outros casos, através dos e-mails, redes sociais, etc.

- *Pornografia infantil*: no Brasil, através do Estatuto da Criança e do Adolescente (art. 240 e seguintes) e do Código Penal (art. 217-A), é punido aquele que expõe a sexualidade infantil em fotos, filmagens, interpretações teatrais, entre outros, e isso é recorrente no meio cibernético.
- *Falsa identidade e falsidade ideológica*: o primeiro acontece quando alguém se passa por uma pessoa que não é, por exemplo, utilizando dados e senhas de pessoa diversa; no segundo caso, a pessoa omite ou insere dados falsos em documentos, prejudicando o direito de terceiros (art.299 e 307 do Código Penal). Assim, na internet esses crimes podem ser cometidos, por exemplo, com a criação de perfis falsos, chamados de “fakes”, nos quais pessoas se passam por outras, inclusive por celebridades.
- *Violação de direitos autorais*: o simples fato de algo estar disponível na internet não quer dizer que é público. Quando uma pessoa utiliza esses dados como se fossem próprios pode estar cometendo um crime e por isso a legislação vigente no país protege a propriedade intelectual, que se divide em propriedade industrial e em direitos autorais, estando dispostos nas Leis nº 9.279/96 e nº 9.609/98 e no Código Penal. Assim, se verifica nestas leis que é crime copiar ou vender produtos sem a autorização do seu verdadeiro proprietário. É considerado crime também a violação dos direitos dos autores de programa, através da venda, aquisição, exposição e ocultação para fins de comércio destes programas.

- *Incitação e apologia ao crime*: as pessoas que estimulam a prática de crimes, que fazem apologia aos criminosos ou aos fatos praticados por eles incorrem nos crimes descritos nos arts. 286 e 287 do CP.

De outro lado estão os chamados *crimes virtuais próprios*, que, como já dito, são aqueles que atingem os sistemas informatizados. Têm inúmeras condutas a serem descritas, mas abordaremos as principais, como¹³:

- *Do vírus e sua disseminação*: nos sistemas modernos um meio de ataque a programas e dados são os *malwares*. Um *malware* bem conhecido é o vírus, que, na verdade, são programas, que tem a capacidade de contaminar sistemas, explorando suas falhas através de e-mails por transmissão de dados maliciosos, o que causa um efeito a depender do grau deste *malware*, podendo dificultar o funcionamento, causar lentidão e até destruir programas e sistemas.

Dentre as várias espécies de vírus estão os *worms* que causam problemas como, lentidão das máquinas, a perda de dados para outros sistemas e podem até possibilitar o controle de um computador de maneira remota.

Estes programas podem causar a uma pessoa danos irreparáveis, pois ela pode vir a perder projetos e pesquisas de uma vida inteira. Mas há também aqueles que são inofensivos, que só servem para diversão de quem os disseminou. Esse tipo de atitude perturba a paz das pessoas, o que corrobora com a ideia de que é necessária a tipificação desses atos, a fim de que sejam punidos os seus responsáveis.

- *Obtenção e transferência ilegal de dados*: um dos ilícitos comuns no mundo informático é a obtenção e transferência ilegal de dados, que pode se dar de diversas formas.

Os *spywares* são os tipos de arquivos utilizados nesta prática, chamados também de programa espião: eles rastreiam todos os tipos de informações do usuário contidas em seu computador.

Estes programas têm versões muito utilizadas para cometer esses delitos que são: os *cookies* e os *trojans* ou *keyloggers*.

¹³ CRESPO, 2011, p. 54-70.

Por violar o direito constitucional que garante à todos a intimidade e privacidade, é uma prática que deve ser penalizada.

- *Acesso não autorizado*: consiste em um ato comum para se chegar a outros delitos. No entanto, ele, por si só, já configura um ilícito, pois o ato de invadir sistemas informáticos alheios (*hacking*), já viola a privacidade da pessoa. Essa conduta tem várias formas de ser praticada desde as mais antigas como a tentativa de obtenção de senhas, até as mais modernas em que o próprio sujeito passivo ao visitar páginas na internet é enganado para conseguir o acesso não autorizado. A tipificação dessa conduta no Brasil seguiria o exemplo de outros ordenamentos jurídicos do mundo.
- *Dano informático*: esse é um crime que gera controvérsias no que diz respeito a necessidade de se criar um tipo penal específico ou não. A dúvida paira, tendo em vista o crime de dano já tipificado no Código Penal brasileiro (art. 163), pois, para alguns juristas é possível a aplicação deste crime quando o fato for praticado contra sistemas informáticos.

Outra corrente, entretanto, posiciona-se em sentido contrário, defendendo a necessidade de criação de uma nova regulamentação. Isso porque, segundo ela, não é possível estender o tipo penal existente, pois a “coisa” que o dispositivo menciona deve ser entendida como bem material e os dados informáticos são na verdade imateriais. Por isso, faz-se necessária a modificação legislativa para estender o art. 163 do CP aos dados informáticos.

- *Divulgação ou utilização indevida de informações*: na internet é rotineira a utilização de dados pessoais dos indivíduos sem autorização para as mais diversas práticas. Essas informações de cunho pessoal devem ser protegidas, isso porque a pessoa fica a mercê de várias situações que podem prejudicá-la. Uma delas é o *spam*, que são mensagens comerciais enviadas a uma massa de indivíduos sem autorização. Essa atitude, além de gerar muito lixo eletrônico, ainda pode causar danos econômicos.

- *Interceptação ilegal de dados*: esta conduta já é coibida pelo ordenamento jurídico brasileiro, que prevê a incriminação daquele que realiza interceptação, seja ela telefônica, temática ou informática sem a autorização judicial ou não obedecendo o que manda a lei (Lei nº 9.096/96, art. 10).
- *Engenharia social e “phishing”*: a engenharia social para o Direito Penal é uma forma de se obter fraudulentamente acesso a informações de terceiros. No meio cibernético isso se configura especialmente pelo *phishing*, que ocorre quando um indivíduo de má-fé através de um e-mail, cartões virtuais, etc., tenta obter dados, como senhas, número de cartão de crédito, entre outros, utilizando-se de falsas pretensões em relação à vítima.

O criminoso, que com essas informações é levado a obter vantagem econômica indevida, incorre nas penas do art. 171 do CP (estelionato), no entanto, somente o fato de enganar o indivíduo para conseguir as informações não é penalmente punível, mesmo sendo necessário.

- *Embaraçamento ao funcionamento de sistemas*: O DOS (Denial of service) é um meio de intervir em sistemas para tirá-los de operação e também a outros computadores ligados à internet, ou seja, retirar do ar sites de grande relevância, o que pode causar grandes prejuízos, tanto quando atinge sites públicos, quanto quando atinge sistemas particulares.

3. AUSÊNCIA DE LEGISLAÇÃO ESPECÍFICA E REPRESSÃO DOS CRIMES INFORMÁTICOS

Com a globalização pela qual o mundo passou nos últimos tempos e o desenvolvimento social da população, a maioria desta já tem acesso à computadores e a internet, o que faz aumentar, cada vez mais, o número de vítimas dos crimes virtuais.

As pessoas têm sido afetadas por estes delinquentes cibernéticos tanto na parte patrimonial, bem como na violação de seu direito à privacidade, à intimidade e à honra, sendo que grande parte desses indivíduos acreditam que esses criminosos ficam impunes.

Assim, o que se coloca em pauta, é a necessidade da abrangência da legislação penal sobre os crimes virtuais, isso porque, apesar de algumas dessas atitudes já serem tipificadas, muitas não o são, o que gera essa impunidade que é verificada quanto a esses tipos de crimes.

No Brasil, os *crimes virtuais impróprios* são punidos com as leis que já existem no ordenamento jurídico brasileiro, tendo em vista que o computador e a internet são somente as ferramentas para o cometimento destes delitos.

A problemática está em relação aos *crimes virtuais próprios*, pois quanto a eles não existem leis que os tipifiquem, e as leis que já se encontram no ordenamento jurídico não poderiam abarcá-los, visto que ocorreria a extensão da norma de forma a prejudicar o autor do fato, o que não é permitido pelo direito brasileiro.

Para se ter uma visão mais clara da necessidade de se criar uma legislação específica, deve-se atentar ao princípio da legalidade, que pode ser encontrado no art. 1º do Código Penal e entre os direitos e garantias fundamentais da Constituição Federal (art. 5º, inciso XXXIX).

Segundo este preceito, não é possível se falar em crime sem uma legislação anterior que o coloque como tal e assim também ocorre em relação às penas. Para o tema tratado, isto quer dizer que, se não forem elaboradas leis para definir como crimes estas condutas praticadas no meio cibernético, o Estado não poderá repreender, através da aplicação de penas, estes criminosos que causam danos a bens jurídicos tutelados pela própria Constituição¹⁴.

O doutrinador Nilo Batista, em sua obra, descreve como característica do princípio da legalidade a possibilidade de seu desdobramento em quatro funções diferentes: proibir a retroatividade da lei penal; proibir a criação de crimes e penas pelo costume; proibir incriminações vagas e indeterminadas; e

¹⁴ LIBERATI, 2009, p. 18.

proibir o emprego de analogia para criar crimes, fundamentar ou agravar penas.¹⁵ Esta última função se aplica ao caso dos crimes virtuais, pois não é possível encaixar todos esses fatos delituosos, nas leis que já existem, uma vez que configuraria analogia “in malam partem”, ou seja, a extensão da norma prejudicaria o autor do fato, o que, segundo Nilo Batista, é reprovado pela doutrina brasileira, nas suas palavras:

Salta aos olhos a total inaplicabilidade da analogia, perante o princípio da legalidade, a toda e qualquer norma que define crimes e comine ou agrave penas, cuja expansão lógica, por qualquer processo, é terminantemente vedada, havendo neste ponto unanimidade na doutrina brasileira.¹⁶

Mesmo com todos estes entraves, ainda existem doutrinadores que apoiam o entendimento de que estas novas leis serviriam apenas para inchar ainda mais a legislação penal já existente e que elas não teriam a aplicabilidade necessária.

Como já foi dito, o mundo se modificou e com essas mudanças aparecem novas ferramentas (computador e internet) que possibilitam a estas pessoas de má-fé a sua utilização para praticar mal feitos. Assim, também o Direito Penal deve se modificar, expandir-se nesta área, visando proteger os bens jurídicos já existentes e estes novos que surgiram, como nos dizeres de Jésus Maria Silva Sanchez:

O Direito Penal é um instrumento qualificado de proteção de bens jurídicos especialmente importantes. Fixado este ponto, parece obrigatório levar em conta a possibilidade de que sua expansão obedeça, ao menos em parte, já a aparição de novos bens jurídicos – de novos interesses ou de novas valorações a interesses preexistentes [...] ¹⁷

Não há dúvida que os interesses relativos ao ciberespaço são novos interesses que decorrem da evolução tecnológica do mundo contemporâneo. São interesses impensáveis pelo Direito Penal clássico e que, portanto, irão requer a ampliação do Direito Penal para que possam ser eficientemente protegidos.

¹⁵ BATISTA, 1996, p. 61-83.

¹⁶ BATISTA, 1996, p. 75.

¹⁷ SÁNCHEZ, 2002, p. 29.

Atento a todas essas dificuldades de se punir os crimes digitais e a maneira como os indivíduos estão sendo lesados faz-se necessária a modernização do Direito penal, com a criação de leis suficientes para punir estes criminosos.

4. AS PRINCIPAIS PROPOSTAS LEGISLATIVAS SOBRE OS CRIMES VIRTUAIS

Por tudo que foi demonstrado ao longo do texto, nota-se que a criação de uma legislação específica é eminente e necessária, mas deve-se ficar atento para que as leis a serem criadas venham realmente para punir as práticas criminosas no ciberespaço, pois como se sabe o Direito Penal é a “ultima ratio”.

O legislador brasileiro, já verificando as mudanças no comportamento criminoso que ocorreram nos últimos anos com a informatização, iniciou a criação de leis para punir os cibercrimes. No entanto, até o momento tais iniciativas não passam de projetos de leis que há muito tempo já tramitam no Poder Legislativo.

Dentre os principais projetos que surgiram nos últimos anos, está a Projeto de Lei (PL) nº 1.713/96 que trata, em seu Capítulo V, dos crimes cometidos nas redes integradas de computadores, como, por exemplo, a incriminação ao acesso indevido. Conjuntamente a este projeto estão apensados outros três: PL nº 2644/96, PL nº 3.258/97 e PL nº 3.692/97. Todos eles discorrem em seu teor sobre os crimes informáticos, como a utilização, reprodução, modificação ou destruição indevida de documento eletrônico. O projeto de lei em pauta já foi arquivado e desarquivado em duas ocasiões, 2007 e 2011.¹⁸

No entanto, essas criações legislativas foram um tanto esquecidas quando foi proposta a PL 84/99, conhecida como “Lei Azeredo”, pois o foco do Poder Legislativo se voltou todo para ele, pois recebeu substitutivo dos

¹⁸ CRESPO, 2011, p. 126-128.

senadores Eduardo Azeredo e Aloízio Mercadante quando tramitou pelo Senado sob o nº 89/03, também denominada como AI-5 digital, fazendo referência ao ato institucional de 1968 da época da Ditadura militar, pois, para muitos, o Senador Azeredo quis impor este projeto. É considerada a principal proposta legislativa sobre estes tipos de crimes. Em seu conteúdo ela prevê tipos penais como, dano a dados e a programas, alteração de senha de acesso a dados e programas, violação de segredo, obtenção indevida de dados, sendo que suas penas variam de 1 a 3 anos.

A PL 89/99 recebeu muitas críticas sobre seu teor mal elaborado e muito abrangente, como do doutrinador Túlio Vianna, que considera ser melhor o arquivamento deste projeto e a criação de um novo com uma melhor técnica penal.¹⁹

O projeto do novo Código Penal (PLS 156/09), que está tramitando no Senado, estabelece em seu Título VI a tipificação dos crimes cibernéticos, do acesso indevido (art. 209), que possui modalidade qualificada e da sabotagem informática (art. 210). Neste texto, ainda se encontram tipificações a esse respeito, na parte que toca aos crimes contra o patrimônio, dano aos dados informáticos (art. 164) e a fraude informática (art. 170) e também nos crimes contra propriedade imaterial que seria a violação de programa de computador (art. 174).

Para aqueles que acompanham os noticiários, é de seu conhecimento que no primeiro semestre deste ano a atriz Carolina Dieckman teve fotos pessoais (nuas) retiradas de seu computador e divulgadas na internet²⁰. Isso impulsionou o Legislativo a propor um novo projeto de lei sobre crimes digitais, a saber, o PL nº 2793/11, do Deputado Federal Paulo Teixeira. Este projeto, inclusive, já passou por votação na Câmara dos Deputados.

Todos estes projetos de leis explanados anteriormente tem um conteúdo razoável para punir estes crimes. No entanto, caminham muito lentamente para a aprovação. Enquanto isso, a impunidade permanece.

¹⁹ VIANNA, 2009.

²⁰ LEMOS, 2012.

CONCLUSÃO

O computador e a internet vieram para facilitar a vida de toda à população, em todos os sentidos, seja no trabalho ou para o lazer: são instrumentos que hoje são indispensáveis ao cotidiano das pessoas. Mas como mencionado durante toda a abordagem do tema, essas ferramentas também servem à indivíduos de má-fé que almejam cometer crimes.

Até o momento, não existem leis específicas que tratam destes crimes informáticos. O que Estado tem feito, é punir estes criminosos quando a prática do crime se encaixa no contexto de um tipo penal já criado por lei (os chamados crimes virtuais impróprios). Para os crimes virtuais próprios, contudo, não há previsão legal.

A dúvida que paira no ar, é se realmente seria necessário criar mais normas para tipificar esses crimes ou não, tendo em vista que o Direito Penal é a última alternativa a se chegar.

Considerando que esses crimes, além de prejudicar os bens jurídicos que já são protegidos, até pela Constituição Federal, trazem consigo novos bens jurídicos para serem defendidos, se faz necessário que Direito Penal se amplie nesta área, e crie novas leis para punir estes delitos virtuais, a fim de proteger toda à população.

O legislador deve criar leis adequadas e suficientes para coibir essas práticas no “ciberespaço”, para que elas não se tornem só mais algumas dentre muitas sem aplicabilidade.

A necessidade dessas novas leis se faz principalmente devido ao princípio da legalidade que rege o ordenamento jurídico brasileiro, pois sem elas essas práticas cibernéticas não serão consideradas crimes e não poderão ser punidas, o que fará crescer a impunidade neste meio.

É necessário atentar para a necessidade urgente da criação legislativa no campo dos crimes virtuais, visando a proteção de todos. No entanto, há diversos projetos de leis sobre esta matéria, que tramitam há anos no Legislativo, devendo suas votações serem priorizadas pelo Congresso, para o país, enfim, ter uma legislação especial sobre o tema.

REFERÊNCIAS BIBLIOGRÁFICAS

BATISTA, Nilo. **Introdução crítica ao direito penal brasileiro**. 3. ed. Rio de Janeiro: Revan, 1996.

BRANDT, Fábio. **Entenda o projeto de lei que estabelece 12 crimes para ações na internet**. Brasília: Net, 2011. Seção Tecnologia. Disponível em: <<http://tecnologia.uol.com.br/ultimas-noticias/redacao/2011/07/02/entenda-o-projeto-de-lei-que-estabelece-12-crimes-para-acoes-na-internet.ihtm>>. Acesso em: 5 out. 2012.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. 1. ed. São Paulo: Saraiva, 2011.

GUIMARÃES, José Augusto Chaves. FURNALETO NETO, Mário. **Crimes na internet: elementos para uma reflexão sobre a ética informacional**. Brasília: Net, 2003. Seção Revista. Disponível em: <<http://www.cjf.jus.br/revista/numero20/artigo9.pdf>>. Acesso em: 16 jul. 2012.

HAMANN, Renan. **A evolução dos computadores**. Curitiba: Net, 2011. Seção Infográfico. Disponível em: <<http://www.tecmundo.com.br/infografico/9421-a-evolucao-dos-computadores.htm>>. Acesso em: 15 jul. 2012.

LEMOS, Marcos. **Novo Projeto de Lei vai regulamentar crimes virtuais: PL 2793/11**. Belo Horizonte: Net, 2012. Seção Assuntos relevantes. Disponível em: <<http://www.ferramentasblog.com/2012/05/novo-projeto-de-lei-regulamentar-crimes-virtuais-pl-2793-11.html>>. Acesso em: 10 out. 2012.

LIBERATI, Maria José Crepaldi Ganancio. Crimes informáticos. 2009. 20 f. Artigo Jurídico (Encontro de iniciação científica) – Faculdade de direito, Faculdades integradas Antônio Eufrásio de Toledo, Presidente Prudente. 2009. Disponível em: <<http://intertemas.unitoledo.br/revista/index.php/ETIC/article/viewFile/2148/2333>> Acesso em: 16 jul. 2012.

PINHEIRO, Emiline Piva. **Crimes virtuais: uma análise da criminalidade informática e da resposta estatal**. 2006. 34 f. Trabalho de conclusão de curso – Faculdade de Direito, Pontifícia Universidade Católica do Rio Grande do Sul. Porto Alegre. 2006. Disponível em: <http://www.pucrs.br/direito/graduacao/tc/tccII/trabalhos2006_1/emeline.pdf> Acesso em: 15 jul. 2012.

SILVA SÁNCHEZ, Jesús-Maria. **A expansão do direito penal: aspectos da política criminal nas sociedades pós-industriais**. Tradução: Luiz Otávio de Oliveira Rocha. 2. ed. São Paulo: Revista dos Tribunais, 2002.

SUA PESQUISA. **História da internet**. Disponível em:
<<http://www.suapesquisa.com/internet/>> . Acesso em: 05 ago. 2012.

TECLAI. Brasil registra 54 crimes virtuais por minuto. Montes Claros: Net, 2012. Seção Notícias Teclai. Disponível em: <
http://www.teclai.com.br/index.php?option=com_content&view=article&id=5909&Itemid=177> . Acesso em: 10 de set. de 2012.

VIANNA, Túlio. **3 críticas ao projeto de lei de crimes informáticos**. Net, 2009. Seção Arquivos diários. Disponível em:
<<http://tuliovianna.org/2009/09/03/3-criticas-ao-projeto-de-lei-de-crimes-informaticos/>> . Acesso em: 5 out. 2012.

WIKIPÉDIA. **Crime informático**. Net, 2012. Disponível em:
<http://pt.wikipedia.org/wiki/Crime_inform%C3%A1tico>. Acesso em: 16 jul. 2012.

WIKIPÉDIA. **História da internet**. Net, 2012. Disponível em: <
http://pt.wikipedia.org/wiki/Hist%C3%B3ria_da_Internet>. Acesso em: 16 jul. 2012.