UNIVERSIDADE DO EXTREMO SUL CATARINENSE – UNESC
PÓS-GRADUAÇÃO ESPECIALIZAÇÃO EM DIREITO PÚBLICO

RENATA BASCHIROTTO VIEIRA

CRIMES DE INFORMÁTICA: AS RECENTES INOVAÇÕES

CRICIÚMA
2014

RENATA BASCHIROTTO VIEIRA

CRIMES DE INFORMÁTICA: AS RECENTES INOVAÇÕES

Monografia apresentada ao Setor de Pós-Graduação da Universidade do Extremo Sul Catarinense – UNESC, para a obtenção do título de especialista em Direito Público.

Orientador: Professor Dr. Cláudio Eduardo Regis de Figueiredo e Silva.

CRICIÚMA
2014

Aos meus pais, pelo apoio incondicional.

AGRADECIMENTOS

A Deus, por me permitir viver com saúde, e sempre amparada por familiares e amigos.

À Universidade do Extremo Sul Catarinense, em especial ao seu corpo docente, que foram diretamente responsáveis pela minha formação acadêmica.

À Escola Superior da Magistratura de Santa Catarina, pela especialização.

Ao meu orientador, Dr. Claudio Eduardo Regis de Figueiredo e Silva, pelo incentivo, auxílio e pronto atendimento a sanar minhas dúvidas.

Aos meus pais, que sempre me apoiaram nas minhas decisões, e dedicam-se, sem medir esforços, em me ajudar a concretizar os meus sonhos.

Aos colegas de classe, com quem eu sanei dúvidas, e também dividi inúmeras insatisfações e aborrecimentos.

“A ciência nunca resolve um problema sem criar pelo menos outros dez”.

George Bernard Shaw

RESUMO

As grandes transformações advindas com a informática, notadamente a internet, certamente trouxeram benfeitorias à sociedade, facilitando o dia-a-dia da população. Paralelamente às inovações, entretanto, surgiram também pessoas que se utilizam da informática para praticar delitos, os criminosos informáticos. Há pouco tempo atrás não existia legislação que tutelasse o sistema informático. Com as recentes inovações legislativas sobre o tema, mostra-se válido o presente estudo.
O objetivo desse trabalho é apresentar alguns aspectos dos crimes cometidos pelo meio da informática e estudar as recentes legislações a respeito.
Este trabalho foi realizado com base em pesquisa bibliográfica.

Palavras-chave: Crime. Informática. Cybercrime.

LISTA DE ABREVIATURAS E SIGLAS

ART. – Artigo

CF – Constituição Federal

CP – Código Penal

CPP – Código de Processo Penal

INC. – Inciso

PL – Projeto de Lei

SUMÁRIO

1 INTRODUÇÃO

O espantoso crescimento da informática nas últimas décadas trouxe grandes benfeitorias para a sociedade como um todo, transformando a vida do homem moderno. A internet apresenta-se como um meio hábil e eficaz de comunicação entre pessoas de diversas partes do mundo, de transmissão de informações, sem contar as inúmeras transações comerciais que se pode fazer por esse meio.

Em contrapartida, essa inovação veio acompanhada também de repercussão no âmbito do Direito Penal e Processual Penal, haja vista que inúmeros crimes e condutas danosas vêm sendo praticados no ambiente virtual.

Até o ano de 2012, não havia tutela penal para o sistema informático. Assim, os atos praticados contra o sistema ficavam isentos de pena, já que somente poderiam ser punidos os delitos com expressa previsão no Código Penal, ou seja, crimes contra o patrimônio, contra a honra, de pedofilia, racismo etc., quando praticados com o auxílio da informática (o agente sequer sai de sua casa para praticar o delito!) eram punidos, mas quando praticados contra o sistema informático (invasão de dispositivo informático) não havia punição.

O objetivo geral desta pesquisa é analisar as recentes inovações sobre os crimes informáticos. Estudar-se-á também os aspectos processuais dos crimes de informática e a tutela penal sobre o tema.

A pesquisa utiliza o método de abordagem dedutivo, partindo dos crimes informáticos para chegar às suas recentes inovações. Possui natureza qualitativa, com método de procedimento monográfico e histórico, sendo a técnica de pesquisa bibliográfica, com base em doutrinas, artigos científicos e legislação.

O trabalho está dividido em três capítulos.

No primeiro capítulo será estudada a evolução da informática e alguns aspectos dos crimes cometidos por meio dela.

O segundo capítulo tratará da tutela penal do sistema informático.

Já no terceiro capítulo será feita uma abordagem da tramitação de dois Projetos de Leis que se transformaram nas mais recentes leis sobre os crimes informáticos.

Como forma de colaboração, pretende a pesquisadora proporcionar à sociedade esclarecimentos sobre o tema, que é bastante corriqueiro, tendo como motivação algumas ocasiões em que teve seu cartão de crédito clonado.

2 DO CRIME DE INFORMÁTICA

2.1 A EVOLUÇÃO HISTÓRICA DA INFORMÁTICA

A Marinha dos Estados Unidos, em conjunto com a Universidade de Harvard, no período da Segunda Guerra Mundial, desenvolveu o computador Harvard Mark I, projetado pelo professor Howard Aiken, com base no calculador analítico de Babbage. Foi daí que nasceram os computadores atuais.[1]

O Computador é um equipamento eletrônico capaz de variados tipos de tratamento automático de informações ou processamento de dados. A máquina pode prover-se de inúmeros atributos, dentre eles o armazenamento/processamento de dados, cálculos em grandes escalas, tratamento de imagens, entretenimento, cultura, etc.[2]

Atualmente estamos na quinta geração[3] de computadores, que tem como principal característica a simplificação e miniaturização do equipamento, além de possibilitar a obtenção de recursos ilimitados, assim como o acesso à rede mundial de computadores.[4]

Registra-se que não há notícias de que o homem, em busca de um equipamento que facilitasse os cálculos matemáticos, tivesse agido com a intenção de lesionar ou colocar em perigo qualquer bem jurídico, mesmo porque as máquinas eram de uso exclusivo de pesquisadores, os quais tinham como objetivo o aperfeiçoamento dela para a obtenção de resultados rápidos e confiáveis que

---

[1] COMPUTADOR, 2014. **Wikipédia**, a enciclopédia livre. Disponível em: < http://goo.gl/2maO >. Acesso em: 26 fev. 2014.

[2] Ibidem.

[3] A primeira geração de computadores surgiu em 1951, e foi caracterizada pelas válvulas eletrônicas; No final dos anos 50, a segunda geração de computadores apresentou os transitores em substituição às válvulas, e nesse período o computador passou a ser utilizado também por civis – até então era de uso científico-militar; Em meados da década de 60, veio a terceira geração de computadores, que passou a se utilizar de circuitos integrados; Com a tecnologia de circuitos integrados em escalas superiores de integração, surgiu a quarta geração de computadores, que se caracterizou pela maior capacidade de armazenamento, rapidez e precisão no desenvolvimento do processamento de dados. SILVA, Rita de Cássia Lopes da. **Direito Penal e Sistema Informático**. São Paulo: Revista dos Tribunais, 2003, p. 18.

[4] Ibidem, p. 19.

viessem a facilitar os seus trabalhos. Os problemas advindos do uso ilícito do computador surgiram quando passaram a fazer parte do cotidiano da população – quando saíram da utilização exclusiva dos cientistas para tornarem-se um equipamento de uso comum.[5]

Segundo Sandra Gouvêa,[6] os primeiros casos de conduta criminosa praticada por meio do uso do computador foram constatados na década de 60, e, por estarem ligados à lesão do patrimônio de alguém, com pretensão de lucro, eram considerados crimes econômicos.

2.2 A INFORMÁTICA E O DIREITO

O direito, por natureza, é conservador, sendo certo que a inovação legislativa é lenta e gradual. Há uma grande distância entre a ordem jurídica e as transformações sociais, e isso não deve ocorrer, sob pena de as leis não serem observadas; Já que o direito eficaz é aquele realmente aplicado e obedecido, o legislador deve acompanhar a evolução social.[7]

As novidades trazidas pela internet atingem o direito em todas as suas áreas. Atualmente, podem-se realizar vários negócios por meio da internet: comprar, vender, trocar, participar de leilões, etc. Profissionais liberais (advogados, psicólogos, etc.) também anunciam seus trabalhos na rede mundial de computadores. Pessoas trabalham e estudam no ambiente virtual. Enfim, tudo pode ser feito de forma prática, sem sair de casa. Estamos na era da informática!

Ao mesmo tempo em que essa evolução facilita o dia-a-dia das pessoas, há quem se utilize do avanço da tecnologia, da internet e do computador, para praticar crimes. Trata-se do criminoso virtual.

---

[5] Ibidem.

[6] *Apud* SILVA, Rita de Cássia Lopes da. Ob. Cit., p. 19.

[7] ELIAS, Paulo Sá. A Tecnologia e o Direito no Século XXI. **Jus Navigandi**, Teresina, ano 6, n. 51, 1 out. 2001. Disponível em: <http://jus.com.br/artigos/2099>. Acesso em: 25 fev. 2014.

2.3 CONCEITOS E NOMENCLATURAS

Crime de informática é um tema atual, e por isso ainda há pouco material publicado na área, sendo várias as nomenclaturas utilizadas: crimes de computador, crimes de internet, crimes informáticos, crimes virtuais, crimes digitais, etc.

Neste trabalho será mencionado sempre "crime de informática", por abranger não só a internet, mas todo o sistema de informática. "Assim, os crimes praticados através da internet são espécies dos crimes de informática, tendo esse último uma área de abrangência maior".[8]

Tal qual a nomenclatura, o conceito de crime de informática também não é uniforme.

Nas palavras de Carla Rodrigues Araújo de Castro:

> Crime de informática é aquele praticado contra o sistema de informática ou através deste, compreendendo os crimes praticados contra o computador e os seus acessórios e os perpetrados através do computador. Inclui-se neste conceito os delitos praticados através da internet, pois pressuposto para acessar a rede é a utilização de um computador.[9]

Para Ivette Senise Ferreira, crime de informática é toda ação típica, antijurídica e culpável contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão.[10]

Já o Professor João Marcello de Araújo conceitua o crime de informática como sendo uma conduta lesiva, dolosa, a qual não precisa, necessariamente, corresponder à obtenção de uma vantagem ilícita, porém praticada sempre com a utilização de dispositivos habitualmente empregados nas atividades de informática.[11]

---

[8] CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. 2 ed. rev. ampl. e atual. Rio de Janeiro: Lúmen Jesus, 2003, p. 8.

[9] Ibidem, p. 9.

[10] FERREIRA, Ivette Senise. **Estudos em Homenagem a Manoel Pedro Pimental**. São Paulo: Revista dos Tribunais, 1992, p. 141-142.

[11] ARAÚJO JUNIOR, João Marcello. **"Computer-crime"**. In: Conferência Internacional de Direito Penal, nº1, Outubro de 1988, Rio de Janeiro. Anais. Rio de Janeiro: Procuradoria Geral da Defensoria Pública, 1988, p. 461.

Marco Aurélio Rodrigues da Costa define crime de informática como todo aquele procedimento que atenta contra dados, que o faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão. Assim, pressupõe dois elementos: contra os dados e também contra o computador, utilizando-se de software e hardware para perpetrá-lo.[12]

Gustavo Testa Corrêa diz que são "os crimes relacionados às informações arquivadas ou em trânsito por computador, sendo esses dados acessados ilicitamente, usados para ameaçar ou fraudar; para tal prática é indispensável a utilização de um meio eletrônico".[13]

Ainda, Angela Bittencourt Brasil não vê diferença no conceito de crime comum e crime de informática, salientando, entretanto, que a fronteira que os separa é a utilização do computador para alcançar e manipular o seu sistema em proveito próprio ou para lesionar outrem.[14]

Isso posto, observa-se que alguns autores utilizam um conceito mais restrito, considerando crimes de informática apenas aqueles praticados contra dados, informações ou *software*, enquanto outros autores se utilizam de um conceito mais amplo, abrangendo a totalidade dos equipamentos utilizados na informática e os crimes cometidos por meio desse sistema.

2.4 CLASSIFICAÇÕES

Os crimes de informática podem ser classificados em crimes próprios e impróprios.

Crimes próprios são aqueles que só podem ser praticados por meio da informática – sem ela é impossível a execução e consumação da infração. Os crimes próprios de informática surgiram com a evolução tecnológica, são tipos novos, que atingem a informática como bem juridicamente protegido, a exemplo da violação de

---

[12] Apud CASTRO, Ob. cit, p. 9.

[13] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. São Paulo: Saraiva, 1999, p. 43.

[14] BRASIL, Angela Bittencourt. **Informática Jurídica – O Ciber Direito** - Rio de Janeiro: edição pessoal, 2000, p. 133-134.

e-mail, pichação de *homepage*, dano em arquivos provocado por envio de vírus, entre outros.[15]

Já os crimes impróprios são os que podem ser praticados de qualquer forma, até mesmo por meio da informática. O agente desse tipo de crime, para cometer o delito utiliza-se do sistema informático. O computador, nesse caso, é um instrumento para executar o crime. São delitos que violam bens já tutelados por nossa legislação, como honra, patrimônio, etc.[16]

Assim, o delito próprio seria aquele que viola o sistema em si, enquanto que no delito impróprio o computador é utilizado apenas como instrumento para atacar qualquer outro bem jurídico tutelado.[17]

Quanto ao objetivo material, há outras classificações, uma delas elaborada por Marco Aurélio Rodrigues da Costa[18]:

> **Crime de Informática Puro**
>
> São aqueles em que o sujeito ativo visa especificamente ao sistema de informática, em todas as suas formas. Entendemos serem os elementos que compõem a informática o *"software"*, o *"hardware"* (computador e periféricos), os dados e sistemas contidos no computador, os meios de armazenamento externo, tais como fitas, disquetes, etc.
>
> Portanto são aquelas condutas que visam exclusivamente a violar o sistema de informática do agente passivo.
>
> As ações físicas se materializam, por exemplo, por atos de vandalismos contra a integridade física do sistema, pelo acesso desautorizado ao computador, pelo acesso indevido aos dados e sistemas contidos no computador.
>
> Portanto, é *crime de informática* puro toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, seja pelo atentado

[15] CASTRO, ob. cit., p. 10.

[16] Ibidem.

[17] FERREIRA, Érica Lourenço de Lima. **Criminalidade Econômica Empresarial e Cibernética**. Florianópolis: Momento Atual, 2004, p. 52.

[18] COSTA, Marco Aurélio Rodrigues da. Crimes de Informática. **Jus Navigandi**, Teresina, ano 2, n. 12, 5 de maio de 1997. Disponível em: <http://jus.com.br/artigos/1826>. Acesso em: 5 de março de 2014.

> físico ou técnico do equipamento e seus componentes, inclusive dados e sistemas.
>
> **Crime de Informática Misto**
>
> São todas aquelas ações em que o agente visa a um bem juridicamente protegido diverso da informática, porém, o sistema de informática é ferramenta imprescindível a sua consumação.
>
> Quando o agente objetiva, por exemplo, realizar operações de transferência ilícita de valores de outrem, em um determinada instituição financeira utilizando-se do computador para alcançar o resultado da vantagem ilegal, e, o computador é ferramenta essencial, defrontamo-nos com um *crime de informática* misto.
>
> É *crime de informática* misto porque incidiriam normas da lei penal comum e normas da lei penal de informática. Da lei penal comum, por exemplo, poder-se-ia aplicar o artigo 171 do Código Penal combinado com uma norma de mau uso de equipamento e meio de informática. Por isso não seria um delito comum apenas, incidiria a norma penal de informática, teríamos claramente o concurso de normas (art. 70, CP).
>
> **Crime de Informática Comum**
>
> São todas aquelas condutas em que o agente se utiliza do sistema de informática como mera ferramenta a perpetração de crime comum, tipificável na lei penal, ou seja, a via eleita do sistema de informática não é essencial à consumação do delito, que poderia ser praticado por meio de outra ferramenta.
>
> Como exemplo, os casos de estelionato (art. 171, CP), e as suas mais amplas formas de fraude. Quando o computador é ferramenta escolhida pelo agente ativo, que poderia escolher outros meios diversos da informática. Porém, é de se pensar na possibilidade de qualificadora para o delito de estelionato o uso do sistema de informática.

Ivette Senise Ferreira[19] divide os crimes de informática em duas categorias. Na primeira delas os delitos são praticados contra o sistema informático (atos contra o computador e atos contra os dados ou programa de computador). Já na segunda categoria, encontram-se os delitos praticados por meio do sistema de informática, que podem ser contra o patrimônio, contra a liberdade individual, propriedade imaterial, etc.

---

[19] Ob. cit., p. 146-152.

Há diversas classificações propostas quanto ao tema em estudo, tendo a pesquisadora se atido a essas por se tratarem das principais.

2.5 SUJEITOS DO CRIME

2.5.1 SUJEITO ATIVO

Toda discussão que se faça acerca da apuração da responsabilidade do conteúdo das informações que passam pela internet decorre do fato de que são vários os agentes que interferem e sustentam esse sistema de rede.[20]

Em princípio, qualquer pessoa pode ser sujeito ativo nos crimes de informática. Por exemplo, um estelionato praticado por meio da internet não requer qualquer qualificação especial do agente. Entretanto, existem alguns delitos que são praticados pelos representantes legais das pessoas jurídicas relacionadas com a rede, a exemplo do provedor de acesso à internet que se recusa, diante de uma ordem judicial, a informar o endereço (IP) de um usuário.[21]

Extrai-se da lição de Fabrízio Rosa[22] que é um engano pensar que os crimes de informática são cometidos apenas por especialistas, pois com a evolução dos meios de comunicação, o aumento de equipamentos, o crescimento da tecnologia e, principalmente, da acessibilidade e dos sistemas disponíveis, qualquer pessoa pode ser um criminoso de informática, o que requer apenas conhecimentos rudimentares. Uma pessoa com o mínimo de conhecimento é potencialmente capaz de cometer crime de informática. É claro que, em regra, o delinquente desse meio é um operador de computadores e de sistemas, mas não se pode generalizar.

Qualquer pessoa, portanto, pode ser sujeito ativo de crime de informática.

---

[20] FERREIRA, Érica Lourenço de Lima. Ob. cit., p. 65.

[21] CASTRO, Carla Rodrigues Araújo de. Ob. cit., p. 11-12.

[22] ROSA, Fabrízio. **Crimes de Informática**. 2 ed. Campinas: Bookseller, 2005, p. 61.

2.5.2 SUJEITO PASSIVO

O sujeito passivo é a pessoa sobre a qual recai a ação ou omissão realizada pelo sujeito ativo. E, em se tratando de crime cometido por meio da informática, o sujeito passivo pode ser qualquer pessoa, física ou jurídica, pública ou privada.

2.6 TEMPO DO CRIME

A descoberta do exato momento em que aconteceu o crime é importante para a aplicação da norma penal, a fim de solucionar o conflito temporal de normas, verificar a imputabilidade do agente, a possibilidade de aplicação de anistia e da prescrição, além da análise das circunstâncias do crime.[23]

Sobre o tempo do crime, mostra-se válido destacarmos três teorias doutrinárias: 1) teoria da atividade ou ação – pela qual o crime é praticado no momento da execução da conduta; 2) teoria do evento ou do resultado – segundo a qual o crime será considerado realizado no momento do seu resultado; 3) teoria mista ou unitária – em que o crime é cometido tanto no momento da conduta quanto no de seu resultado.[24]

O Brasil adotou a teoria da ação ou atividade, conforme o art. 4° do Código Penal: “Considera-se praticado o crime no momento da ação ou omissão, ainda que outro seja o momento do resultado”.

Nos delitos informáticos em geral o período de tempo entre a ação e o resultado muitas vezes é grande. Isso porque, quando o agente digita determinado comando em um computador ligado em rede, para que ele execute uma operação em outro computador, esse comando passará por muitos cabos até chegar ao seu destino. Como exemplo, temos o caso em que o criminoso quer transferir todos os dados do computador da vítima para o seu – essa operação pode levar horas, mas o

---

[23] VIANNA, Túlio Lima. **Fundamentos de Direito Penal Informático.** Belo Horizonte. Disponível em: <http://goo.gl/860lJQ>. Acesso em: 12 mar. 2014.

[24] Ibidem.

delito será considerado praticado no momento em que o agente digitou o comando para iniciar a transferência.[25]

2.7 LUGAR DO CRIME

A determinação do lugar em que o crime ocorreu é fundamental para verificar a competência – se a lei brasileira será ou não aplicada.

Sobre o lugar do crime, há três teorias, a saber:

> Teoria da atividade: o crime ocorre no lugar em que foi praticada a ação ou omissão, ou seja, a conduta criminosa [...];
> Teoria do resultado: o crime ocorre no lugar em que ocorreu o resultado [...];
> Teoria da ubiquidade: também conhecida por teoria mista, já que para esta teoria, o crime ocorre tanto no lugar em que foi praticada a ação ou omissão (atividade), como onde se produziu, ou deveria se produzir o resultado (resultado).[26]

O Código Penal Brasileiro adotou, em seu art. 6°, a teoria da ubiquidade (ou mista): "Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado". [27]

A aplicação desta norma nos casos dos crimes praticados por meio da internet quando o computador que o criminoso se utiliza para atingir a vítima encontra-se em outro país é simples quando em ambos os países o fato é considerado típico.

O problema é quando o fato é típico apenas em um dos países envolvidos - pode ocorrer que a conduta seja típica no país em que o comando é dado, porém atípica onde se dá o resultado fático. Ou, ao contrário.[28]

---

[25] Ibidem.

[26] RISTOW, Rogério. **Lei Penal no Espaço:** Lugar do Crime. Disponível em: <http://goo.gl/yFMqd8>. Acesso em: 12 mar. 2014.

[27] BRASIL. Decreto-lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Rio de Janeiro.

[28] VIANNA, Túlio Lima. Ob. Cit.

Para que haja punição, nesse caso, é necessário que o fato seja típico em ambas as legislações dos países envolvidos, sob pena de ofensa direta ao princípio constitucional do *nullum crimen sine lege*.[29]

Túlio Lima Vianna[30] finaliza a questão dizendo:

> Raciocinar de forma contrária é admitir a paradoxal hipótese de um crime que não obedece a norma estabelecida no art. 6º do CP, pois só seria crime no local da conduta ou no do resultado, sendo no outro conduta lícita.

2.8 INVESTIGAÇÃO

Sobre a investigação criminal, leciona Carla Rodrigues Araújo de Castro[31]:

> A investigação tem por finalidade fornecer subsídios para que o titular da ação penal possa ingressar em juízo, devendo a Autoridade Policial buscar identificar autoria e materialidade da infração. Assim, a investigação tem dois focos: o primeiro é de descobrir se o crime realmente existiu, e em caso positivo, quais foram as suas circunstâncias; o segundo é esclarecer quem praticou a conduta.

Consta no art. 6° do Código de Processo Penal um rol exemplificativo das diligências a serem efetuadas, cabendo à Autoridade Policial determinar outras que se amoldam ao caso em concreto.

Em se tratando de crimes de informática, a investigação não é muito diferente da dos crimes comuns, sendo que apenas se acrescenta os instrumentos investigatórios advindos com o computador e a internet. Assim, o delegado pode orientar-se pelos critérios enumerados no dispositivo legal supracitado, ouvindo o ofendido, indiciado, testemunhas, etc.[32]

Várias situações podem surgir nos crimes praticados por meio da informática: crimes cometidos através de *e-mail*, praticados em sites, fraudes, desvios, pedofilia, etc. Na primeira hipótese, se o agente enviou um *e-mail* contendo

---

[29] Ibidem.

[30] Ibidem.

[31] Ob. cit., p. 105.

[32] CASTRO, Carla Rodrigues Araújo de. Ob. cit., p. 105.

ameaça a outrem, o destinatário sabe o endereço eletrônico do "agressor", assim como o provedor utilizado. Com isso, bastaria apenas que a Autoridade Policial procedesse à intimação do provedor para que fornecesse os dados do computador do usuário, como nome, qualificação e endereço.[33]

Já quando a infração é praticada por meio de um *site*, a Autoridade Policial deve identificar quem é a pessoa cadastrada como responsável pela página. Em outros casos, possuindo informações de data e horário exato utilizado pelo usuário, com auxílio de um técnico, o Delegado também pode chegar ao autor da infração.[34]

Há inúmeras formas de se praticar um crime informático, assim é essencial que o investigador, para obter sucesso em seu trabalho, chegue até a ferramenta que os criminosos usaram para a prática do crime. A "ferramenta" pode ser a utilização de programas maliciosos, *e-mail*, *websites*, programas de transferência de informações, grupos de debate, redes sociais, sites de comércio eletrônico, entre inúmeros outros. Identificado o meio utilizado, diversas são as técnicas para se chegar à autoria.[35]

O problema é que há meios de burlar o endereço de IP, o que dificulta em muito o trabalho da investigação. Isso porque quem está cometendo um crime via internet provavelmente está ciente de que pode ser facilmente descoberto caso tenha o seu IP cadastrado corretamente. É por isso que os criminosos utilizam-se de *lan houses*, *cyber* cafés, redes de *wi-fi* abertas, ou até mesmo de documento falso em cadastro. Logo, os investigadores devem estar atentos a esses detalhes.[36]

Não bastasse isso, pessoas utilizam-se do *proxy*[37], que oculta o verdadeiro IP utilizado em um evento de internet, dificultando o rastreamento de

---

[33] Ibidem, p. 105-106.

[34] Ibidem, p. 106.

[35] CAVALCANTE, Waldek Fachinelli. Crimes cibernéticos: noções básicas de investigação e ameaças na internet. **Jus Navigandi**, Teresina, ano 18, n. 3782, 8 nov. 2013. Disponível em: <http://jus.com.br/artigos/25743>. Acesso em: 6 mar. 2014.

[36] Ibidem.

[37] ***Proxy*** é um servidor intermediário que atende a requisições repassando os dados do cliente à frente: um usuário (cliente) conecta-se a um servidor *proxy*, requisitando algum serviço, como um arquivo, conexão, página *web*, ou qualquer outro recurso disponível no outro servidor.

quem realizou a conduta. Os servidores *proxy*, portanto, acabam por facilitar o anonimato na internet, embora eles não tenham somente fim ilícito.[38]

Ainda sobre o assunto investigação, com o objetivo de transformar a internet em um ambiente ético e responsável, que permita às crianças, jovens e adultos criarem, desenvolverem e ampliarem relações sociais, conhecimentos e exercerem a plena cidadania com segurança e tranquilidade, um grupo de cientistas da computação, professores, pesquisadores e bacharéis em Direito fundaram, em dezembro de 2005, uma associação civil de direito privado, sem fins lucrativos, chamada "SaferNet Brasil", visando combater crimes e violações aos direitos humanos na internet.[39]

A Associação SaferNet Brasil possui um site, onde tem um canal que se pode fazer denúncias sobre crimes contra direitos humanos na internet, dentre eles os crime de pornografia infantil, racismo, apologia e incitação a crimes contra a vida, xenofobia, neonazismo, maus tratos contra animais, intolerância religiosa, homofobia e tráfico de pessoas.[40]

Contam também com um canal de atendimento ao público, chamado "helpline.br". Nesse canal, podem-se receber orientações pontuais e informativas para esclarecer dúvidas, ensinar formas seguras de uso da internet, e também orientar crianças e adolescentes, assim como seus próximos, que vivenciaram situações de violência *on-line* (humilhações, intimidações, chantagens, tentativa de violência sexual ou exposição forçada em fotos ou filmes sensuais, etc). Quem faz a orientação *on-line* é uma equipe de psicólogos[41].

Um servidor *proxy* pode, opcionalmente, alterar a requisição do cliente ou a resposta do servidor e, algumas vezes, pode disponibilizar este recurso mesmo sem se conectar ao servidor especificado. Pode também atuar como um servidor que armazena dados em forma de cache em redes de computadores. São instalados em máquinas com ligações tipicamente superiores às dos clientes e com poder de armazenamento elevado.
Esses servidores têm uma série de usos, como filtrar conteúdo, providenciar anonimato, entre outros. Disponível em: <http://pt.wikipedia.org/wiki/Proxies> Acesso em 07/03/2014.

[38] CAVALCANTE, Waldek Fachinelli. Ob. cit.

[39] Disponível em: <http://www.safernet.org.br/site/institucional>. Acesso em 6 mar. 2014.

[40] Canal para oferecer denúncias: <http://www.safernet.org.br/site/denunciar>. Acesso em 6 mar. 2014.

[41] Canal "helpline.br": <http://www.safernet.org.br/site/webline>. Acesso em 6 mar. 2014.

Hoje, conforme consta no site da Associação SaferNet Brasil, há 11 Delegacias Especializadas em Crimes Cibernéticos, distribuídas entre o Distrito Federal e os estados de Espírito Santo, Goiás, Mato Grosso do Sul, Minas Gerais, Pará, Paraná, Pernambuco, Rio de Janeiro, Rio Grande do Sul e São Paulo.

2.9 COMPETÊNCIA

A competência é a delimitação da jurisdição, ou seja, o espaço dentro do qual pode determinada autoridade judiciária aplicar o direito aos litígios que lhe forem apresentados, compondo-os.[42]

Antes de ficar estabelecida a competência para processar e julgar os crimes cometidos pelo meio da informática é necessário verificar a incidência ou não da lei brasileira, utilizando-se, para tanto, do lugar onde o crime ocorreu.

Sendo o Brasil o país competente, deve ser aplicada a determinação contida no art. 70 do Código de Processo Penal, segundo a qual a competência é determinada, em regra, pelo lugar em que se consumar a infração ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução.[43]

2.10 PROVA PERICIAL

A perícia é um meio de prova que “consiste em um exame elaborado por pessoa, em regra profissional, dotada de formação e conhecimentos técnicos específicos, acerca de fatos necessários ao deslinde da causa”. Trata-se de um juízo de valoração científico, artístico, contábil, avaliatório ou técnico, exercido por um especialista, com o intuito de prestar ajuda ao juiz em questões que não fazem parte da sua área de conhecimento.[44]

---

[42] NUCCI, Guilherme de Souza. **Manual de Processo Penal e Execução Penal**. 3ª ed. rev., atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2007, p. 225.

[43] BRASIL. Decreto-lei nº 3.689, de 3 de outubro de 1941. **Código de Processo Penal**. Rio de Janeiro.

[44] CAPEZ, Fernando. **Curso de Processo Penal**. 7. Ed, revista e ampliada. São Paulo: Saraiva, 2001, p. 264.

De acordo com o art. 158 do Código de Processo Penal, “quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado”.

Em regra, os crimes de informática são infrações não transeuntes, ou seja, deixam vestígios. Assim, o corpo de delito deve ser submetido à análise de perícia, que deverá ser feita por pessoa que contenha conhecimento técnico sobre informática, programação e internet. O perito deverá informar ao magistrado o tipo de equipamento utilizado no cometimento da infração, os programas instalados no computador, entre outras considerações que reputar importantes.[45]

2.11 *E-MAIL* COMO PROVA DE CONDUTA DELITUOSA

A palavra “e-mail” tem origem americana, vindo da expressão “eletronic mail”, que possui alguns significados, podendo ser entendida como correio eletrônico, endereço eletrônico e correspondência eletrônica. Neste trabalho será utilizada a última acepção da palavra, na qual *e-mail* é uma carta virtual digitada no computador e enviada por um programa ou *site* específico – é uma troca de informações por meio da informática.[46]

Na obra “Vocabulário Jurídico”, de De Plácido e Silva, verifica-se que a expressão correspondência “indica todos os meios de comunicação escrita que possam por em ligação duas pessoas distantes, na intenção de manterem uma troca de ideias ou de vontades entre si”.[47]

O *e-mail* é, portanto, um tipo de correspondência.

O artigo 5º, inciso XII, da Constituição Federal[48] dispõe sobre a inviolabilidade das correspondências:

> É inviolável o sigilo da correspondência e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei

[45] CASTRO, Rita Rodrigues Araújo de. Ob. cit., p. 114.

[46] Ibidem, p. 117.

[47] Rio de Janeiro: Forense, 1990, p. 573.

[48] BRASIL. **Constituição da República Federativa do Brasil**, de 5 de outubro de 1988. Brasília, disponível em: <http://goo.gl/HwJ1Q>. Acesso em: 7 mar. 2014.

> estabelecer para fins de investigação criminal ou instrução processual penal.

Como se vê, o texto constitucional não excepciona a inviolabilidade da correspondência. Assim, a princípio, o sigilo é absoluto.

A Lei nº 9.296/96[49] disciplina a interceptação de comunicações telefônicas, abrangendo sua eficácia para os fluxos de comunicações em sistemas de informática e telemática. A sindicância é permitida nos casos de apuração de infrações penais, desde que seja o único meio de prova, necessitando, todavia, de autorização judicial:

> Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.
>
> Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.

Segundo Carla Rodrigues Araújo de Castro, devemos considerar que "a telemática é uma ciência que cuida da manipulação de dados e informações, conjugando o computador com meios de comunicação, conclui-se que a lei atinge os e-*mails"*.[50]

Assim, podemos concluir que, desde que observadas as regras da Lei nº 9.296/96, será admitida a utilização do *e-mail* como prova, na seara penal, uma vez que feita a interceptação judicial, a correspondência eletrônica terá valoração de prova legítima a ser utilizada no processo criminal.

2.11.1 VALOR DO E-MAIL COMO PROVA

Conforme acima exposto, o *e-mail* pode ser admitido em sede de direito penal como prova, então passamos a analisar a sua valoração como tal.

---

[49] BRASIL. Lei nº 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. **Lei da Interceptação Telefônica**. Brasília, Disponível em: <http://goo.gl/CByup>. Acesso em: 7 mar. 2014.

[50] CASTRO, Carla Rodrigues Araújo de. Ob. Cit., p. 118.

No julgamento do valor da prova, como disse certa vez o Ministro Mário Guimarães, "exercita o juiz os seus conhecimentos de ordem geral e atua com os atributos que lhe são pessoais de perspicácia, de bom senso, de objetividade, de homem experiente".[51]

O magistrado, portanto, é livre para valorar a prova, formar sua convicção, devendo fundamentar sua decisão, deixando explícitos os motivos que o levaram a creditar mais valor a certa prova.

Sobre o assunto, prevê o art. 155 do Código de Processo Penal:

> O juiz formará sua convicção pela livre apreciação da prova produzida em contraditório judicial, não podendo fundamentar sua decisão exclusivamente nos elementos informativos colhidos na investigação, ressalvadas as provas cautelares, não repetíveis e antecipadas.

Não existe valor predeterminado para nenhum tipo de prova. O magistrado fará a valoração de acordo com seus princípios, e precedido de contraditório, sempre que possível.

O *e-mail*, como o DNA e fotos, é um exemplo de prova inominada, já que não está previsto expressamente no Código de Processo Penal[52], mas não por essa razão deve ter um "desvalor" inicial. Certamente, em alguns casos o juiz pode entender que o *e-mail* não tem total credibilidade, entretanto também é certo que em outras oportunidades o *e-mail* pode ser prova cabal para decisão de uma causa.[53]

O fato é que a tecnologia vem atropelando o Direito e sem demora "nos brindará com meios mais seguros de transmissão, bem como de identificação dos autores das mensagens", por meio da assinatura digital. Logo, muito em breve será antiquada a argumentação de fragilidade dos *e-mails* como meio de prova.[54]

---

[51] Apud REIS, Nazareno César Moreira. **A relativização do ônus da prova e a Justiça Constitucional:** uma breve reflexão sobre a concretização de valores constitucionais em face da inércia legislativa. Jus Navigandi, Teresina, ano 7, n. 92, 3 out. 2003. Disponível em: <http://goo.gl/K6Tfiv>. Acesso em: 7 mar. 2014.

[52] PENTEADO FILHO, Nestor Sampaio. Provas ilícitas e investigação criminal. **Jus Navigandi**, Teresina, ano 7, n. 56, 1 abr. 2002. Disponível em: <http://jus.com.br/artigos/2843>. Acesso em: 7 mar. 2014.

[53] CASTRO, Carla Rodrigues Araújo de. Ob. cit., p. 127.

[54] Ibidem.

3 A TUTELA PENAL INFORMÁTICA

3.1 BEM JURÍDICO E DENOMINAÇÃO LEGAL

Segundo Temístocles Telmo Ferreira Araújo[55], bem jurídico pode ser conceituado como algo que tenha "relevância para a sociedade, implicando em um juízo positivo de valor acerca de uma determinada situação social para o desenvolvimento humano".

E continua, aduzindo que não basta o reconhecimento da importância do bem jurídico para que ele seja tutelado, as ofensas e as condutas praticadas em seu desfavor devem ser relevantes, a ponto de lesá-lo gravemente ou deixá-lo em iminente perigo de lesão. Como resposta a essas ofensas é que o legislador penal tornará a conduta criminalizada.[56]

A técnica legislativa determina que os nomes dos delitos devam ter como base o bem jurídico por ele tutelado. Nesse sentido, leia-se o ensinamento de Heleno Cláudio Fragoso[57]:

> A classificação dos crimes na parte especial do código é questão de técnica legislativa, e é feita com base no bem jurídico tutelado pela lei penal, ou seja, a objetividade jurídica dos vários delitos ou das diversas classes de intenções.

Esse também é o pensamento de Jair Leandro Lopes[58]:

> No CP brasileiro, os crimes são distribuídos, a partir do art. 121, por Títulos, Capítulos e Seções, de acordo com o chamado critério da objetividade jurídica, isto é, de conformidade com a natureza do bem ou objeto jurídico contra o qual se dirigiu a ação do agente. Assim, temos crimes "contra a pessoa", "crimes contra o patrimônio" e mais nove Títulos, cada qual referindo-se a um bem ou valor, considerado merecedor da reforçada proteção jurídico penal.

---

[55] ARAÚJO, Temístocles Telmo Ferreira. **Bem jurídico e os limites da tutela penal**. Jus Navigandi, Teresina, 2013. Disponível em: <http://goo.gl/ZL0lUH>. Acesso em: 12 mar. 2014.

[56] Ibidem.

[57] Apud VIANNA, Túlio Lima. **Fundamentos de Direito Penal Informático.** Belo Horizonte. Disponível em: <http://goo.gl/860lJQ>. Acesso em: 12 mar. 2014.

[58] Apud VIANNA, Túlio Lima. Ob. Cit.

Sendo assim, Túlio Lima Vianna aponta que a denominação “delito virtual” é totalmente inadequada, pois não há sentido em se falar de um bem jurídico virtual, restando, então, duas opções viáveis: delito informático ou computacional.[59]

A terminologia mais precisa para os delitos em estudo é “crimes informáticos”, por basear-se no bem jurídico penalmente tutelado, que é a inviolabilidade das informações automatizadas (dados).[60]

3.2 ASPECTOS GERAIS SOBRE LEGISLAÇÕES APLICADAS À INFORMÁTICA

As transformações advindas da informática trouxeram grandes benfeitorias à sociedade, facilitando o dia-a-dia da população em diversas atividades. Em contrapartida, indivíduos mal intencionados passaram a se utilizar da internet – e da informática em geral – para praticarem crimes.

Sobre o computador, escreveu Felipe de Senna Silva Araújo:

> [...] a máquina tanto pode ser alvo de tentativas de corrupção, destruição ou subtração de informações nela contidas, através de spywares, phishing ou outros meios, quanto pode ser a própria ferramenta do crime, quando é utilizada, por exemplo, para a divulgação ou fomento da pornografia infantil, invasões ou criações de perfis falsos em sites de relacionamento da internet, fraudes bancárias e ao comércio eletrônico, ou violações a segredos industriais e profissionais. Soma-se a todos estes ilícitos a violação aos direitos autorais de programas de computador, que possui lei específica para condenar, a até 4 (quatro) anos de reclusão, aqueles que praticam a pirataria de software.[61]

Num primeiro momento, foi detectado o problema da pirataria (reprodução de *software*), e, em 1987, surgiu a Lei da Informática – Lei 7.646, assim denominada porque “foi a primeira a tipificar uma conduta que, embora assemelhada à violação de direito autoral, constituía um crime informático em sentido próprio, tendo

---

[59] Ob. Cit.

[60] Ibidem.

[61] **Crimes Cibernéticos:** novos desafios do Direito Penal. 2009. Disponível em: <http://goo.gl/QmTbK>. Acesso em: 10 mar. 2014.

declarado expressamente que o regime de proteção à propriedade intelectual de programas do computador era o *direito do autor*".[62]

Depois de vários projetos de lei e muitos debates, a Lei 7647/87 acolheu a tese que já era vencedora no plano internacional, proclamando, no seu art. 2°, o direito de autor sobre os programas de computador [...], além de tipificar também a sua comercialização indevida.[63]

Nesse mesmo entendimento seguiu a atual Lei da Informática – Lei n° 9.609/98, que dispõe sobre a proteção da propriedade intelectual do programa de computador, no sentido de que o regime de proteção é aquele conferido às obras literárias pela legislação de direitos autorais e conexos vigente no país.[64]

Sobre a citada lei, em um artigo intitulado "A Ideologia da Propriedade Intelectual: a inconstitucionalidade da tutela penal dos direitos patrimoniais de autor", Túlio Lima Vianna faz profunda crítica à tutela penal dos direitos patrimoniais do autor, discorrendo acerca das vantagens da cópia de sua obra:

> [...] somente ao proprietário cabe o direito de alienar (doar, permutar ou vender) a coisa, pelo óbvio motivo de que ao fazê-lo perderá os direitos de dela usar e fruir. O autor, porém, nada perde com a cópia da sua obra. Pelo contrário, quanto mais pessoas lerem seus textos, ouvirem sua música e apreciarem a sua arte, tanto mais reputação ganhará na sociedade.
> A obra intelectual, como seu próprio nome indica (lat. *opèra,ae* ´´trabalho manual´´), não é, pois, uma espécie de propriedade, mas simplesmente "trabalho intelectual". A invenção da "propriedade intelectual" nas origens do sistema capitalista teve a função ideológica de encobrir esta sua natureza de "trabalho".[65]

Ao final, aduz que se deve declarar inconstitucional a tutela penal dos direitos patrimoniais de autor, [...] seja pela inobservância do princípio constitucional da taxatividade, seja pela inobservância da vedação constitucional à prisão por

---

[62] LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coordenadores) e outros. **Direito & Internet – Aspectos Jurídicos Relevantes**. 1 ed. Bauru, SP: EDIPRO, 2001, p. 226.

[63] Ibidem, p. 227.

[64] BRASIL. Lei nº 9.609, de 19 de fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9609.htm>. Acesso em: 10 mar. 2014.

[65] VIANNA, Túlio Lima. A ideologia da propriedade intelectual: a inconstitucionalidade da tutela penal dos direitos patrimoniais de autor. **Jus Navigandi**, Teresina, ano 11, n. 1174, 18 set. 2006. Disponível em: <http://jus.com.br/artigos/8932>. Acesso em: 10 mar. 2014.

dívidas. E conclui, dizendo que "entender de forma diversa é consagrar a instrumentalização do Direito Penal como meio de coerção ao pagamento de dívidas civis e de intervenção econômica para a garantia de monopólios privados".[66]

Com a chegada da internet, os fatos que já possuíam tipificação legal e bem jurídico tutelado pelo ordenamento penal (patrimônio, honra, etc) ficaram vistos apenas como uma nova instrumentalização da modalidade delitiva. Entretanto, novas condutas que lesionam os direitos e garantias da sociedade vão além dos bens jurídicos que já estavam tutelados pelo Direito Penal, a exemplo do dano informático, violação ao dispositivo informático e outros. Assim, quando ocorria alguma ofensa a esses bens, pela falta de previsão legal, nada se podia fazer, já que o Direito Penal não tipifica condutas por analogia, com fundamento no princípio da legalidade, previsto no art. 5 º, inc. XXXIX, da CF: "Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal".[67]

A tutela penal para esses casos era necessária!

Antes da entrada em vigor da Lei 12.737/2012, que ensejou um novo tipo penal (invasão de dispositivo informático) e algumas alterações no Código Penal, existiam outros projetos de lei que visavam tutelar o mesmo bem jurídico.

Dentre esses projetos, estava o de n. 84/99, do Deputado Luiz Piauhylino, que chegou a tramitar por mais de 12 anos no Congresso Nacional. O PL desencadeou vários debates jurídicos sobre o seu conteúdo, tendo recebido inúmeras críticas dos militantes das redes sociais, que chegaram a formular uma petição online, intitulada "Pelo veto ao projeto de cibercrimes – Em defesa da liberdade e do progresso do conhecimento da internet brasileira, contrária à sua aprovação, com mais de 160 mil assinaturas. Por suprimir a liberdade de expressão dos internautas e enquadrar na tipificação penal até um simples *download*[68], o projeto ficou conhecido como "AI-5 Digital".[69]

---

[66] Ibidem

[67] 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: 11 mar. 2014.

[68] O uso mais comum do termo *download* está relacionado com a obtenção de conteúdo da Internet, onde um servidor remoto hospeda dados que são acessados pelos clientes através de aplicativos específicos, como é o caso dos navegadores. De fato, o acesso de qualquer informação na Internet (como uma página da web, por exemplo) é feito através do download prévio de seu conteúdo (texto,

Em sua redação original, o PL 84/99 contou com mais de vinte artigos, tipificando várias condutas como crime, mas acabou se materializado na Lei 12.735/2012[70], que trouxe apenas duas modificações de natureza processual: 1) agregou à Lei de Crimes Contra Raça e Cor (Lei 7.716/89) a possibilidade de ordem judicial, ainda antes do inquérito policial, para a cessação de transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio, de cunho racista; 2) previsão da necessidade de estruturação dos órgãos da polícia judiciária, com setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

No ano de 2011 foi aprovado pela Câmara dos Deputados outro projeto de lei, o PL n. 2793/2011, que foi apresentado pelos Deputados Paulo Teixeira, Luiza Erundina, Manuela Dávila, João Arruda, Brizola Neto e Emiliano José justamente para combater o Projeto de Lei n 84/99, considerado, à época, defasado e excessivo.

Esse novo projeto, ao contrário do anterior, amparou somente bem jurídico ainda não tutelado pelo Direito Penal. Ainda assim, houve grande discussão acerca dele, discussão essa que só teve fim com a publicação, na internet, de fotos da atriz Carolina Dieckmann. Ela foi vítima de *crackers*[71], que conseguiram invadir seu computador e obter sua senha de e-mail, e de posse da senha tiveram acesso a

---

imagens, etc) e posterior exibição do conteúdo que se encontra localmente disponível no dispositivo. No entanto, o uso comum (não-técnico) do termo *download* se limita a referenciar o conteúdo que é obtido da internet para visualização posterior (offline), como um documento ou aplicativo. *In*: DOWNLOAD, 2014. **Wikipédia**, a enciclopédia livre. Disponível em: < http://goo.gl/BdL7PP >. Acesso em: 12 mar. 2014.

[69] THOMAZ, Paula. **O AI-5 digital.** 2011. Carta Capital. Disponível em: <http://goo.gl/1RrxG>. Acesso em: 11 mar. 2014.

[70] BRASIL. **Lei nº 12.735**, de 30 de novembro de 2012. Disponível em: < http://goo.gl/DRl4Vd >. Acesso em: 12 mar. 2014.

[71] *Cracker* é o termo usado para designar o indivíduo que pratica a quebra (ou *cracking*) de um sistema de segurança, de forma ilegal ou sem ética. Este termo foi criado em 1985 por hackers em defesa contra o uso jornalístico do termo *hacker*. O uso deste termo reflete a forte revolta destes contra o roubo e vandalismo praticado pelo *cracking*. In CRACKER, 2014. **Wikipédia**, a enciclopédia livre. Disponível em: <http://pt.wikipedia.org/wiki/Cracker>. Acesso em: 11 mar. 2014.

diversas fotos da atriz seminua e em posições em que expunha sua intimidade. As fotos disseminadas pelos *crackers* foram parar até em sites pornográficos.[72]

Os responsáveis por invadir o computador da atriz foram presos e com eles foram apreendidos os computadores e demais instrumentos do crime. À época, o PL 2793 ainda não havia sido transformado em Lei e os criminosos acabaram sendo indiciados por furto.[73]

O crime de furto, previsto no art. 155 do Código Penal, trata da subtração de coisa alheia móvel. O bem móvel remete a algo material, que possa ser tocado, e por isto soa no mínimo estranho que os agentes tenham sido enquadrados nesse delito, já que a ação deles estava relacionada a bem jurídico imaterial; a conduta violou a intimidade e imagem da atriz.[74]

Foi a partir dos fatos envolvendo a atriz que os parlamentares agilizaram a tramitação do PL 2793, o qual foi transformado na Lei 12.737[75], sancionada em 30 de novembro de 2012. A lei ficou conhecida por "Lei Carolina Dieckmann".

Essa lei fez poucas alterações no Código Penal, incluindo dois artigos (154-A e 154-B) e alterando a redação dos arts. 266 e 298 do mesmo diploma legal.

O art. 154-A do CP trouxe um grande avanço, tutelando o dispositivo informático. Vejamos:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no **caput**.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações

---

[72] Thomaz, Paula. Ob. Cit.

[73] Ibidem.

[74] Ibidem.

[75] BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <http://goo.gl/PeDjn>. Acesso em: 12 mar. 2014.

> sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Analisando o artigo supracitado, Sandro Costa criticou o *caput* do dispositivo, em especial porque a pena para a figura simples desse delito é de detenção, e por isso a principal diligência para comprovação da infração é vedada: não cabe interceptação da comunicação telemática, por se tratar de infração apenada com detenção (cf. art. 2°, inc. III, da Lei 9.296/96).[76]

Asseverou ainda que, em princípio, diante do dolo específico mencionado no artigo, fica afastada a criminalização da conduta do agente que pratica a simples invasão de dispositivo informático sem as finalidades especificadas.[77]

O art. 154-B dispõe sobre a ação penal para o caso de crime de invasão de dispositivo informático. De acordo a determinação legal, a ação será pública condicionada à representação, salvo no caso de crime cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos, quando a ação penal será pública incondicionada.

Quanto ao art. 266 do CP, houve o acréscimo de um parágrafo, considerando crime o fato de interromper serviço telemático ou de informação de utilidade pública, ou impedir/dificultar o seu restabelecimento. Essa figura alcança os ataques a sites governamentais por crackers, “que tiram do ar” o servidor do site.

---

[76] COSTA, Sandro. **Novos cibercrimes nas Leis 12.735 e 12.737.** 2012. Disponível em: < http://goo.gl/kAY1Pq >. Acesso em: 12 mar. 2014.

[77] Ibidem.

A última alteração da citada lei foi no tocante ao art. 298 do CP: o cartão de crédito ou débito foi equiparado a documento particular. Agora a clonagem de cartões de crédito ou débito é criminalizada por meio desse dispositivo.

A Lei 12.737/2012 inovou o cenário jurídico penal, apresentando resposta às pretensões da população, que presenciava o acontecimento de certas condutas lesivas no ambiente virtual, mas nada podia fazer, em face da ausência de tipificação penal.[78]

Anota-se, entretanto, que a citada lei não tem o condão de acabar com os crimes praticados na internet, já que presenciamos constante evolução tecnológica, sendo certo que a legislação tende a não acompanhar a possível chegada de novas condutas lesivas a bens considerados relevantes para uma sociedade moderna.[79]

Dito isso, resta evidente que a inovação do criminoso informático requer mais que uma Lei regulamentando condutas delituosas. Mostra-se necessário uma preparação apropriada dos órgãos da justiça penal e das forças policiais para essa tarefa, que deve contar com agentes que detenham alto conhecimento na área da computação, pois nada adianta a criação de uma lei se não houver atuação conjunta do Poder Judiciário, Ministério Público e das polícias civil e federal para melhor regulamentá-la.[80]

Ivette Senise Ferreira conclui:

> [...] não somente devem os órgãos de segurança poder contar com pessoal treinado e qualificado para a investigação especializada que esse tipo de criminalidade requer, mas também devem eles ser dotados de equipamentos modernos, de alta tecnologia, aptos para enfrentar a engenhosidade de infratores que apresentam um tipo criminológico diferente do infrator comum. Para isso devem os investigadores serem treinados de molde a entender o funcionamento dos sistemas informáticos e as ações invasivas dos criminosos virtuais, que muitas vezes são profissionais ou pessoas com conhecimentos técnicos que facilitam a sua atuação e dificultam a descoberta".[81]

---

[78] ROCHA, Carolina Borges. Ob. Cit.

[79] Ibidem.

[80] Ibidem.

[81] In LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coordenadores) e outros. Ob. Cit., p. 234.

4 AS RECENTES INOVAÇÕES LEGISLATIVAS NA ÁREA DA INFORMÁTICA

4.1 DA TRAMITAÇÃO DOS PROJETOS DE LEI N° 84/1999 E 2793/2011 NO CONGRESSO NACIONAL

Primeiramente, cumpre esclarecer que todos os dados históricos referentes a este capítulo foram extraídos do endereço eletrônico da Câmara dos Deputados.[82]

4.1.1 DO PROJETO DE LEI N° 84/1999

Preocupado com a ausência de lei que regulasse os crimes cometidos por meio da informática, o então Deputado Luiz Piauhylino apresentou, em 24 de fevereiro de 1999, o Projeto de Lei n° 84, dispondo sobre os crimes cometidos na área da informática, suas penalidades e outras providências.

Em sua justificativa para apresentação do Projeto de Lei, o parlamentar anotou que na legislatura anterior o Deputado Cassio Cunha Lima havia apresentado o PL n° 1713/96, tratando sobre o acesso, a responsabilidade e os crimes cometidos nas redes integradas de computadores. Mencionou que referido projeto foi distribuído, inicialmente, à Comissão de Ciência e tecnologia, Comunicação e Informática, tendo como relator a sua pessoa, sendo que após a realização de audiência pública e debates *on-line* não houve tempo suficiente para que o substitutivo fosse apresentado durante aquela legislatura, razão pela qual o PL restou arquivado.

O Projeto de Lei n° 84/99 contou com quatro capítulos e dezoito artigos, nos quais o Deputado discorreu sobre os princípios reguladores da prestação de serviço por rede de computadores, o uso de informações disponíveis em computadores ou rede de computadores, dos crimes de informática (dano a dado ou

---

[82] Câmara dos Deputados. **Projeto de Lei n° 84**, de 24 de fevereiro de 1999. Elaborado pelo Deputado Luiz Piauhylino. Disponível em: <http://goo.gl/YO9FQ>. Acesso em: 10 mar. 2014; e **Projeto de Lei n° 2793**, de 29 de novembro de 2011. Elaborado pelos Deputados Paulo Teixeira, Luiza Erundina, Manuela Dávila, João Arruda, Brizola Neto e Emiliano José. Disponível em: <http://goo.gl/ePUCC>. Acesso em: 10 mar. 2014.

programa de computador; acesso indevido ou não autorizado; alteração de senha ou mecanismo de acesso a computador ou dados; obtenção indevida ou não autorizada de dados ou instrução de computador; violação de segredo armazenado em computador, meio magnético, de natureza magnética, óptica ou similar; criação, desenvolvimento ou inserção em computador de dados ou programa de computador com fins nocivos; e veiculação de pornografia através de rede de computadores) e suas penalidades.

Encaminhado à Comissão de Ciência e Tecnologia, Comunicação e Informática, o Deputado Marcelo Barbieri, então relator, votou, em 9 de junho de 1999, pela aprovação do projeto de Lei 84/99 nos termos firmados pelo autor do PL, e, em reunião ordinária realizada no dia 30 de junho de 1999, a Comissão aprovou o parecer favorável do relator.

Em 2 de julho de 1999, o projeto foi remetido à Comissão de Constituição e Justiça e de Redação, e distribuído ao Deputado Léo Alcântara (em 29/03/2000), o qual, como relator, destacou o desamparo que se encontra nossa sociedade, que reclama providências legislativas na área de crimes de computador, apontando, em especial, a dificuldade ou impossibilidade de punir ações ilícitas praticadas por meio da informática ou contra o sistema de informação, votando, ao final, pela constitucionalidade, juridicidade, boa técnica legislativa, e no mérito pela aprovação do projeto, nos termos do Substitutivo que apresentou.

No Substitutivo apresentado, o parlamentar procedeu à adequação das penas impostas no PL, em consonância com o Código Penal, reduzindo-as. Eliminou um conjunto de circunstâncias qualificadoras repetidas, previstas para cada um dos crimes, incluindo-as em um único artigo, dispondo sobre a sua aplicação a todos os crimes ali tipificados. Discorreu sobre a importância de o projeto ter iniciativa para introdução de lei extravagante, ao invés de elencar os crimes no bojo do Código Penal[83], e fez outras retificações quanto à redação, alteração na ordem dos artigos e supressão de artigos.[84]

---

[83] Embora fosse recomendável elencar no bojo do Código Penal os crimes de que trata este projeto, afigura-se correta a iniciativa para introdução de lei extravagante. Isso ocorre porque a proposição trata também de assuntos que não poderiam ser inseridos naquele Código. Desse modo, somente em legislação esparsa poderemos ver tipificadas as condutas criminosas relativas à informática.

[84] [...] note-se que, em nosso Código Penal, a quantidade da pena *in abstracto* vem especificada simultaneamente em números e por extenso e, ainda, que a Lei Complementar determina, em seu

No dia 6 de novembro de 2000, o relator da Comissão de Relações Exteriores e de Defesa Nacional, Deputado Abelardo Lupion, emitiu parecer favorável à aprovação do PL, com Substitutivo.

Em reunião deliberativa ordinária, realizada no dia 15 de maio de 2002, a Comissão de Constituição e Justiça e de Redação aprovou, por unanimidade, o parecer do relator com o Substitutivo.

O projeto seguiu para apreciação da Comissão de Segurança Pública e Combate ao Crime Organizado, tendo o Deputado Nelson Pellegrino, como relator, emitido parecer, em dezembro de 2002, pela aprovação do PL n° 84/99, com proposta de Substitutivo, contemplando os mesmos objetivos do projeto, mas em vez de Lei esparsa, inseriu as transformações na legislação existente (Código Penal e Lei 9.296/96).[85] A Comissão opinou pela aprovação do Substitutivo apresentado pelo Deputado.

---

art. 11, II, f, que qualquer referência a número ou percentual deve ser feita por extenso. Por tal motivo, modificamos a redação das penas previstas.
Alteramos a ordem dos artigos que tratam dos crimes, para que a seqüência refletisse a ordem provável dos atos de um agente desse tipo de crime, bem como uma possível gradação da gravidade dos delitos cometidos.
Finalmente, sugerimos a supressão dos arts. 14 e 18, com a conseqüente renumeração dos demais.
O art. 14 regulamentava a veiculação de material pornográfico em rede de computadores. Considerando o uso intensivo que atualmente crianças e adolescentes fazem do computador, cujo uso se encontra cada vez mais associado a atividades educativas e culturais, não há porquê transformá-lo em meio de divulgação de pornografia. O controle do acesso ao computador por usuários menores de idade é mais difícil do que o controle do conteúdo divulgado, sendo, portanto, mais produtivo proibir a veiculação de material pornográfico do que o acesso a ele.
O art. 18 contraria a norma constitucional consagrada no art. 84, IV, que estabelece como competência privativa do Presidente da República a regulamentação das leis. Conseqüentemente, ao estabelecer prazo ao Poder Executivo para realização de tal tarefa, está avançando na sua competência constitucional. Realmente, não faria sentido o Legislativo impor a duração desse processo, pois este envolve tratamento de detalhes de operacionalização que são da alçada exclusiva do Executivo, que sobre eles tem melhor compreensão, de vez que os gerencia. Nesse sentido já se pronunciou o Supremo, em sede de ação direta de inconstitucionalidade, declarando a inconstitucionalidade de se assinalar tal prazo.

[85] [...] Estamos propondo, desse modo, um Substitutivo, que contempla os mesmos objetivos dos Projetos analisados e atualiza a legislação no que concerne às novas condutas delituosas, praticadas com o uso das recentes tecnologias.
Entretanto, em vez de Lei esparsa, estamos inserindo essas transformações no Código Penal e na Lei nº 9.296, de 1996.
Assim esperamos contribuir com o aprimoramento do sistema normativo, ao mesmo tempo em que resguardamos o espírito das proposições apresentadas e aqui analisadas.

No mês de novembro de 2003, realizou-se sessão deliberativa do Plenário da Câmara dos Deputados, sendo aprovado o Substitutivo apresentado pela Comissão de Segurança Pública e Combate ao Crime Organizado, restando prejudicados o projeto inicial e o substitutivo da Comissão de Constituição e Justiça e de Redação.

Aprovada a redação final, a matéria foi encaminhada ao Senado Federal para apreciação, em 12 de novembro de 2003.

Em 16 de julho de 2008, o então Deputado Julio Semeghini, juntamente com outros líderes partidários, solicitou urgência para apreciação do Projeto de Lei nº 84, de 1999.

Na data de 18 de julho de 2008, o Senado Federal aprovou, em revisão, o Projeto de Lei enviado pela Câmara, apresentando Substitutivo, contendo vinte e três artigos, os quais dispuseram de novas tipificações penais, além de obrigações administrativas aos provedores de acesso à Internet.

Com a revisão do Senado Federal, que optou por incluir os crimes eletrônicos e suas respectivas punições no Código Penal, Código Penal Militar e na legislação penal esparsa, afastando a ideia inicial de criar uma lei específica disciplinando a matéria, o Projeto retornou à Câmara dos Deputados, em agosto de 2008, para apreciação do Substitutivo apresentado pelo Senado.

Já na Câmara dos Deputados, o Substitutivo foi encaminhado às Comissões de Ciência e Tecnologia, Comunicação e Informática; Segurança Pública e Combate ao Crime Organizado, e Constituição e Justiça e de Cidadania.

Em 19 de agosto de 2008, a sociedade requereu realização de audiência pública para debate do PL.[86]

Os Deputados Pinto Itamaraty e Paulo Henrique Lustosa, por intermédio das Comissões de Segurança Pública e Combate ao Crime Organizado e da Ciência e Tecnologia, Comunicação e Informática, solicitaram realização de audiência pública para debater a tipificação de crimes e delitos cometidos na área de informática e suas penalidades.

Em 5 de agosto de 2010, o então relator da Comissão de Segurança Pública e Combate ao Crime Organizado, Deputado Pinto Itamaraty, asseverou que

---

[86] O requerimento pode ser visto no seguinte *link*:<http://goo.gl/Yx4GA0>. Acesso em 21 fev. 2014.

o Substitutivo apresentado pelo Senado Federal veio a melhorar o Projeto de Lei do Deputado Piaulyno, que estava desatualizado pelo passar do tempo, votando, ao final, pela aprovação do projeto.[87]

O Deputado Regis de Oliveira, relator da Comissão de Constituição de Justiça e de Cidadania apresentou extenso parecer[88], no dia 25 de janeiro de 2011, posicionando-se pela aprovação do Substitutivo apresentado pelo Senado, mas com vinte de uma emendas supressivas e uma aglutinativa.

Os deputados Emiliano José, Luiza Erundina e Pinto Itamaraty também postularam a realização de audiência pública para discussão do PL.

No dia 16 de maio de 2012, o relator da Comissão de Ciência e Tecnologia, Comunicação e Informática, Deputado Eduardo Azeredo, emitiu parecer pela aprovação do Substitutivo apresentado pelo Senado Federal, com algumas considerações.[89]

Já em Plenário, a Comissão de Segurança Pública e Combate ao Crime Organizado emitiu parecer ao Substitutivo do Senado Federal, proferido pelo relator Deputado Otavio Leite, que concluiu pela aprovação do PL na forma do Parecer da Comissão de Ciência e Tecnologia, Comunicação e Informática.[90]

De igual modo, o Deputado Sibá Machado, relator da Comissão de Constituição e Justiça e de Cidadania, também em plenário, concluiu pela constitucionalidade, juridicidade e técnica legislativa; e, no mérito, pela aprovação do PL na forma do Parecer da Comissão de Ciência e Tecnologia, Comunicação e Informática.

_____

[87] Inteiro teor do parecer do Deputado Pinto Itamaraty: <http://goo.gl/8iqPNt>. Acesso em 21 fev. 2014.

[88] Parecer completo disponível em: <http://goo.gl/x25fvD>. Acesso em 21 fev. 2014.

[89] a) Pela rejeição do artigo 9º do Substitutivo do Senado Federal para manter o artigo 7º do texto original do Projeto de Lei nº 84, de 1999, aprovado pelo Plenário da Câmara dos Deputados em novembro de 2003;
b) Pela aprovação dos artigos 15, 18 e 19 do Substitutivo do Senado;
c) Pela aprovação da ementa do substitutivo, exceto as expressões “de rede de computadores, ou” e “dispositivos de comunicação ou”;
d) Pela aprovação do artigo 1º, exceto as expressões “de rede de computadores, ou” e “dispositivos de comunicação ou”;
e) Pela rejeição dos artigos 2º, 3º, 4º, 5º, 6º, 7º, 8º, 10º, 11, 12, 13, 14, 16, 17, 20, 21 e 22.

[90] Inteiro teor do parecer do Deputado Eduardo Leite: <http://goo.gl/p6IUCY>. Acesso em 21 fev. 2014.

Em 7 de novembro de 2012 o plenário aprovou a redação final do Projeto de Lei n° 84/1999[91], encaminhando a matéria à sanção.

Finalmente, após quase treze anos de tramitação no Congresso Nacional, o Projeto de Lei n° 84/1999 foi transformado na Lei Ordinária n° 12.735/2012[92], sendo vetado parcialmente.[93]

4.1.2 DO PROJETO DE LEI N° 2793/2011

Em 29 de novembro de 2011, os Deputados Paulo Teixeira, Luiza Erundina, Manuela Dávila, João Arruda, Brizola Neto e Emiliano José apresentaram no Plenário da Câmara dos Deputados o Projeto de Lei n° 2793/2011.

O citado PL dispunha sobre a tipificação criminal de delitos informáticos, notadamente a invasão de dispositivo informático, alterando o Código Penal e dando outras providências.

Em sede de justificativa, os Deputados mencionaram serem inegáveis os avanços trazidos à sociedade por meio do uso da internet e das novas tecnologias, bem como a necessidade, por conta desses avanços, da regulamentação de aspectos relativos à sociedade da informação, objetivando assegurar os direitos dos cidadãos e garantir que a utilização dessas tecnologias possa ser potencializada em seus efeitos positivos e minimizada em seus impactos negativos; Fizeram uma breve abordagem sobre o PL n° 84/99, enfatizando a impossibilidade de emendá-lo ou alterá-lo, por conta de questões regimentais, diante do seu avançado estágio de tramitação, razão pela qual deram início ao Projeto de Lei ora estudado; Citaram algumas diferenças entre os Projetos de Lei n° 84/99 e 2793/2011, e, por fim, analisaram especificamente os tipos penais que propuseram.[94]

---

[91] Redação final do Projeto de Lei n° 84/99: <http://goo.gl/JCfDhZ>. Acesso em 21 fev. 2014.

[92] Íntegra da Lei 12.735/2012: <http://goo.gl/cAC95V>. Acesso em 21 fev. 2014.

[93] Mensagem de veto: <http://goo.gl/TidPXS>. Acesso em 21 fev. 2014.

[94] A íntegra da justificativa apresentada pelos Deputados está disponível em: <http://goo.gl/X7qvFT>. Acesso em 25 fev. 2014.

O PL tramitou em regime de urgência, com base no art. 155 do Regimento Interno da Câmara dos Deputados.[95]

Aprovada a Redação Final[96] do Projeto de Lei n° 2793/2011, assinada pelo Relator Deputado Nelson Pellegrino em 15 de maio de 2012, a matéria foi encaminhada ao Senado Federal para apreciação.

Ainda no mês de maio do ano de 2012 a atriz Carolina Dieckmann teve mais de trinta imagens suas seminua divulgadas na internet, tendo recebido ameaças de extorsão, para pagamento de dez mil reais, a fim de que as fotos não fossem publicadas na rede mundial de computadores.

Carolina registrou boletim de ocorrência a respeito do fato, e a Polícia, após investigações e a prisão dos agentes criminosos, descartou a hipótese de as imagens terem sido copiadas de uma câmera fotográfica levada para conserto. Constatou-se que a caixa de e-mails da atriz havia sido violada por *crackers.*[97]

O fato teve grande repercussão nacional, sendo citado nas redes de televisões, jornais de grandes circulação e sites.

No dia 5 de novembro de 2012, a Mesa da Câmara dos Deputados recebeu ofício do Senado Federal, comunicando a aprovação do PL em revisão, com Substitutivo, e no dia seguinte as Emendas do Senado[98] foram encaminhadas às Comissões de Segurança Pública e Combate ao Crime Organizado e Constituição e Justiça e de Cidadania.

Em Sessão Deliberativa Extraordinária realizada no dia 7 de novembro de 2012, na Câmara dos Deputados, o Deputado Sibá Machado, Relator da Comissão de Segurança Pública e Combate ao Crime Organizado, emitiu parecer pela

_____

[95] Art. 155. Poderá ser incluída automaticamente na Ordem do Dia para discussão e votação imediata, ainda que iniciada a sessão em que for apresentada, proposição que verse sobre matéria de relevante e inadiável interesse nacional, a requerimento da maioria absoluta da composição da Câmara, ou de líderes que representem esse número, aprovado pela maioria absoluta dos Deputados [...].

[96] A Redação Final do Projeto n° 2793/2011, antes de a matéria seguir ao Senado Federal, pode ser visualizada neste *link*: <http://goo.gl/3uVzyO>. Acesso em 25 fev. 2014.

[97] Fonte: <http://goo.gl/Mrjjq4>. Acesso em 25 fev. 2014.

[98] As Emendas apresentadas pelo Senado Federal podem ser vistas na íntegra no endereço: <http://goo.gl/s1FzK5>. Acesso em 25 fev. 2014.

aprovação das Emendas n° 1 (com acréscimo de uma expressão), 2 e 3, e pela rejeição das Emendas n° 4 e 5.[99]

O Relator da Comissão de Constituição e Justiça e de Cidadania, Deputado Fabio Trad, concluiu pela constitucionalidade, juridicidade e técnica legislativa do PL, e, no mérito, pela aprovação das Emendas n° 1 (com acréscimo de uma expressão), 2 e 3, e pela rejeição das Emendas n° 4 e 5.[100]

As Emendas n° 1, 2 e 3 do Senado Federal foram aprovadas pelo Plenário da Câmara dos Deputados, nos termos dos pareceres dos relatores das Comissões acima mencionadas, e rejeitadas as Emendas n° 3 e 4.

Aprovada a redação final[101], o PL foi encaminhado à sanção no dia 9 de novembro de 2012.

Em 30 de novembro de 2012, pouco mais de um ano após a sua apresentação, o Projeto de Lei n° 2793/2011 foi transformado na Lei Ordinária n° 12.737, a qual ficou conhecida como “Lei Carolina Dieckmann”.

---

[99] A íntegra do parecer do Deputado Sibá Machado está disponível em: <http://goo.gl/UbtjOr>. Acesso em 25 fev. 2014.

[100] A íntegra do parecer do Deputado Fabio Trad pode ser vista neste link: <http://goo.gl/81in87>. Acesso em 25 fev. 2014.

[101] Redação final do PL n° 2793/2011: <http://goo.gl/kUp6k3>. Acesso em 25 fev. 2014.

5 CONCLUSÃO

O avanço tecnológico ocorrido na área da informática e o uso massivo da Internet por importante parcela da sociedade propiciaram o surgimento de novos tipos penais, bem como novas formas de praticar crimes já conhecidos. Fácil a percepção de que a informática se tornou um meio eficaz para execução de tipos penais.

Foi dessa forma que nasceu o denominado “crime de informática”, objeto de estudo deste trabalho, sendo conceituado como aquele praticado contra ou por meio do sistema informático.

Através da pesquisa bibliográfica realizada, denota-se tratar de um assunto extremamente atual, podendo-se perceber que a legislação acerca da informática era bastante escassa em nosso país.

As Leis 12.735 e 12.737, ambas de 2012, inovaram o cenário jurídico penal, respondendo à aflição da sociedade e dos aplicadores da lei, que presenciavam condutas lesivas ao homem acontecerem no ambiente virtual, mas nada podiam fazer, haja vista a falta de previsão legal, ficando os agentes criminosos isentos de pena.

Hoje, o ordenamento jurídico existente em nosso país tutela as principais condutas indesejadas, mesmo praticadas no ambiente virtual, embora ainda a legislação se encontre defasada e de certa forma destoada da realidade.

É importante anotar que as leis não têm o condão de acabar com os crimes informáticos. A progressão da criminalidade informática requer outras providências por parte do Estado, dirigidas à sua apuração e repressão de forma eficaz.

Há evidente necessidade de preparação apropriada das forças policiais e dos órgãos da justiça penal para reprimir esses crimes, que exige pessoal qualificado e treinado para a investigação especializada. E não é só isso. Os profissionais precisam ter à sua disposição equipamentos modernos, aptos a enfrentar a destreza de infratores que apresentam um tipo criminológico diferente do infrator comum, infratores esses que muitas vezes são profissionais da área informática ou pessoas com apurado conhecimento técnico, que facilitam a sua atuação e dificultam a sua identificação.

Além disso, como forma de prevenção, é preciso investir na instalação de equipamentos de segurança nos próprios computadores, a fim de evitar o ataque de invasores ou o dano à programas, a exemplo do que aconteceu com a atriz Carolina Dieckmann.

O fato é que sempre estaremos a mercê dos criminosos, devendo nos precaver da forma que nos é possibilitada.

REFERÊNCIAS

ARAÚJO, Felipe de Senna Silva. **Crimes Cibernéticos**: novos desafios do Direito Penal. 2009. Disponível em: < http://goo.gl/QmTbK >. Acesso em: 10 mar. 2014.

ARAÚJO JUNIOR, João Marcello. **"Computer-crime"**. In: Conferência Internacional de Direito Penal, nº1, Outubro de 1988, Rio de Janeiro. Anais. Rio de Janeiro: Procuradoria Geral da Defensoria Pública, 1988.

ARAÚJO, Temístocles Telmo Ferreira. **Bem jurídico e os limites da tutela penal**. Jus Navigandi, Teresina, 2013. Disponível em: < http://goo.gl/ZL0lUH >. Acesso em: 12 mar. 2014.

BRASIL, Angela Bittencourt. **Informática Jurídica – O Ciber Direito**. Rio de Janeiro: edição pessoal, 2000.

BRASIL. **Constituição da República Federativa do Brasil**, de 5 de outubro de 1988. Brasília, disponível em: < http://goo.gl/HwJ1Q >. Acesso em: 7 mar. 2014

____. Decreto-lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Rio de Janeiro, disponível em: < http://goo.gl/ncXtw >. Acesso em: 11 mar. 2014.

____. Decreto-lei nº 3.689, de 3 de outubro de 1941. **Código de Processo Penal**. Rio de Janeiro, disponível em: < http://goo.gl/tpNxl >. Acesso em: 11 mar. 2014.

____. Lei nº 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. **Lei da Interceptação Telefônica**. Brasília, disponível em: < http://goo.gl/CByup >. Acesso em: 7 mar. 2014.

____. **Lei nº 9.609**, de 19 de fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9609.htm>. Acesso em: 10 mar. 2014.

____. **Lei nº 12.735**, de 30 de novembro de 2012. Disponível em: < http://goo.gl/DRl4Vd >. Acesso em: 12 mar. 2014.

____. **Lei nº 12.737**, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: < http://goo.gl/PeDjn >. Acesso em: 12 mar. 2014.

Câmara dos Deputados. **Projeto de Lei n° 84**, de 24 de fevereiro de 1999. Elaborado pelo Deputado Luiz Piauhylino. Disponível em: < http://goo.gl/YO9FQ >. Acesso em: 10 mar. 2014.

____. **Projeto de Lei n° 2793**, de 29 de novembro de 2011. Elaborado pelos Deputados Paulo Teixeira, Luiza Erundina, Manuela Dávila, João Arruda, Brizola Neto e Emiliano José. Disponível em: < http://goo.gl/ePUCC >. Acesso em: 10 mar. 2014.

CAPEZ, Fernando. **Curso de Processo Penal**. 7. Ed, revista e ampliada. São Paulo: Saraiva, 2001.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. 2 ed. rev. ampl. e atual. Rio de Janeiro: Lúmen Jesus, 2003.

CAVALCANTE, Waldek Fachinelli. **Crimes cibernéticos**: noções básicas de investigação e ameaças na internet. Jus Navigandi, Teresina, ano 18, n. 3782, 8 nov. 2013. Disponível em: < http://jus.com.br/artigos/25743 >. Acesso em: 6 mar. 2014.

COMPUTADOR, 2014. **Wikipédia**, a enciclopédia livre. Disponível em: < http://goo.gl/2maO >. Acesso em: 26 fev. 2014.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. São Paulo: Saraiva, 1999.

COSTA, Marco Aurélio Rodrigues da. **Crimes de Informática**. Jus Navigandi, Teresina, ano 2, n. 12, 5 de maio de 1997. Disponível em: <http://jus.com.br/artigos/1826>. Acesso em: 5 de março de 2014.

COSTA, Sandro. **Novos cibercrimes nas Leis 12.735 e 12.737.** 2012. Disponível em: < http://goo.gl/kAY1Pq >. Acesso em: 12 mar. 2014.

CRACKER, 2014. **Wikipédia**, a enciclopédia livre. Disponível em: <http://pt.wikipedia.org/wiki/Cracker >. Acesso em: 11 mar. 2014.

DE PLACIDO, Silva e. **Vocabulário Jurídico**. Rio de Janeiro: Forense, 1990.

DOWNLOAD, 2014. **Wikipédia**, a enciclopédia livre. Disponível em: < http://goo.gl/BdL7PP >. Acesso em: 12 mar. 2014.

ELIAS, Paulo Sá. **A Tecnologia e o Direito no Século XXI**. Jus Navigandi, Teresina, ano 6, n. 51, 1 out. 2001. Disponível em: <http://jus.com.br/artigos/2099>. Acesso em: 25 fev. 2014.

FERREIRA, Ivette Senise. **Estudos em Homenagem a Manoel Pedro Pimental**. São Paulo: Revista dos Tribunais, 1992.

FERREIRA, Érica Lourenço de Lima. **Criminalidade Econômica Empresarial e Cibernética**. Florianópolis: Momento Atual, 2004.

JESUS, Damásio E. de. **Direito Penal**: Parte Geral. v.1. 28 ed. rev. e atual. São Paulo: Saraiva, 2005.

LEI 'Carolina Dieckmann', que pune invasão de PC's, entra em vigor. 2013. Disponível em: < http://goo.gl/Mrjjq4 >. Acesso em: 25 fev. 2014.

LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coordenadores) e outros. **Direito & Internet – Aspectos Jurídicos Relevantes**. 1 ed. Bauru, SP: EDIPRO, 2001.

NUCCI, Guilherme de Souza. **Manual de Processo Penal e Execução Penal**. 3ª ed. rev., atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2007.

PENTEADO FILHO, Nestor Sampaio. **Provas ilícitas e investigação criminal**. Jus Navigandi, Teresina, ano 7, n. 56, 1 abr. 2002. Disponível em: < http://jus.com.br/artigos/2843 >. Acesso em: 7 mar. 2014.

REIS, Nazareno César Moreira. **A relativização do ônus da prova e a Justiça Constitucional**: uma breve reflexão sobre a concretização de valores constitucionais em face da inércia legislativa. Jus Navigandi, Teresina, ano 7, n. 92, 3 out. 2003. Disponível em: < http://goo.gl/K6Tfiv >. Acesso em: 7 mar. 2014.

RISTOW, Rogério. **Lei Penal no Espaço:** Lugar do Crime. Disponível em: < http://goo.gl/yFMqd8 >. Acesso em: 12 mar. 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: 11 mar. 2014.

ROSA, Fabrízio. **Crimes de Informática**. 2 ed. Campinas: Bookseller, 2005.

SAFERNET BRASIL. **Associação SaferNet**. Disponível em: < http://goo.gl/oCTkb >. Acesso em: 6 mar. 2014.

SILVA, Rita de Cássia Lopes da. **Direito Penal e Sistema Informático**. São Paulo: Revista dos Tribunais, 2003.

THOMAZ, Paula. **O AI-5 digital**. 2011. Carta Capital. Disponível em: < http://goo.gl/1RrxG >. Acesso em: 11 mar. 2014.

VIANNA, Túlio Lima. **A ideologia da propriedade intelectual**: a inconstitucionalidade da tutela penal dos direitos patrimoniais de autor. Jus Navigandi, Teresina, ano 11, n. 1174, 18 set. 2006. Disponível em: < http://jus.com.br/artigos/8932 >. Acesso em: 10 mar. 2014.

____. **Fundamentos de Direito Penal Informático.** Belo Horizonte. Disponível em: < http://goo.gl/860lJQ >. Acesso em: 12 mar. 2014.