

CRIMES DE INFORMÁTICA: CONCEITO, CLASSIFICAÇÃO, PRINCÍPOS E O TRATAMENTO DADO PELO DIREITO PENAL BRASILEIRO.¹

Cristal Yasmim de Oliveira Xavier Jardim²

Professor Orientador: Lincoln Rufino³

RESUMO

O surgimento da Internet e o progresso tecnológico, incontestavelmente trouxeram inúmeros benefícios. Mas juntamente com essas inovações, nasceu também uma nova classe de delinquentes que passou a utilizar o computador para cometer crimes. Muitas das condutas aqui capituladas, embora conhecidas, ainda não estão tipificadas como crime. O fato é que o Direito não foi capaz de acompanhar os avanços do mundo digital, e a carência de legislação tornou impraticável a penalização dos sujeitos ativos em determinadas situações, visto que nossa lei não pune ato sem que antes haja uma previsão legal. O presente artigo expõe um estudo acerca do tratamento dado pelo Direito Penal Brasileiro aos chamados Crimes de Informática, a necessidade de uma lei específica para conduzir essa esfera virtual, análise dos sujeitos do crime e um comparativo com a legislação de outros países.

Palavras-chave: Crimes. Crimes de informática. Direito Penal. Internet. Legislação.

ABSTRACT

The emergence of the Internet and technological progress undoubtedly brought many benefits. But along with these innovations, was also born a new class of offenders who started to use the computer to commit crimes. Many of these behaviors mentioned here, although known, are still not typified as a crime. The fact is that the law was not able to follow the progress of the digital world, and the lack of legislation became impractical penalty of active subjects in certain situations, as our law does not punish without first act there is a legal provision. This article presents a study of treatment given by the Brazilian Criminal Law to the so-called Crimes Computing, the need for a specific law to conduct this virtual realm, analysis of the subject of crime and a comparison with the laws of other countries.

Keywords: Crimes. Computer Crimes. Criminal Law. Internet. Legislation.

¹ Artigo apresentado como pré-requisito para obtenção do grau de Bacharel em Direito pelo Centro Universitário do Rio Grande do Norte – UNI-RN.

² Acadêmica do curso de Direito do Centro Universitário do Rio Grande do Norte – UNI-RN.

³ Mestre e orientador do Curso de Direito do Centro Universitário do Rio Grande do Norte – UNI-RN.

1.0 INTRODUÇÃO

A motivação para realizar o presente trabalho deve-se às consequências do avanço tecnológico no âmbito criminal e penal, destacando a deficiência do nosso Ordenamento Jurídico em relação ao tema.

Os benefícios trazidos pela internet são incontestáveis. Ela se apresenta como a ferramenta mais poderosa de comunicação. Entretanto, junto aos benefícios, a era digital também deu origem aos crimes de informática, possibilitando o surgimento de novas condutas ilícitas, bem como a existência de outras maneiras de execução de crimes já conhecidos.

Dispondo o art.5º, XXXIX, da Constituição Federal, “não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal”. Logo, constata-se que para “alguém ser punido e responsabilizado penalmente, é necessário que a lei descreva, prévia e minuciosamente, todos os elementos do ato considerado ilícito praticado pelo agente.” (SILVA,2003,p.15).

Isto posto, é necessário que as ações praticadas através de computadores, realizadas mediante o uso da Internet, estejam figuradas em lei para que possam ser penalizadas.

Assim ratifica Sandro D'Amato Nogueira (2009):

O sentimento de impunidade na Internet é evidente, e, é quase que absoluta a falta de punição para alguns crimes, isso justamente pela falta de uma lei que regule todo esse mundo digital. Quase todo crime virtual hoje tem que ter sua conduta adaptada ao nosso Código Penal de 1940, daí umas das dificuldades principais das nossas autoridades em processar, condenar, prender, e manter preso um acusado de delito informático.

Vários países já moldaram suas leis acerca deste assunto. A Itália, por exemplo, agregou 15 novas leis ao seu Código Penal relativas à criminalidade na informática.

Observa-se, portanto, que no Brasil, há uma carência de legislação específica capaz de conduzir o contexto virtual que nos cerca. O Direito deve acompanhar e se adaptar à sociedade da informação. Dentre as poucas leis que se prontificam a tratar do assunto, destacam-se a Lei 9.609/98, que aduz sobre a proteção da propriedade intelectual de programa de computador e sua

comercialização e a Lei 9.983/00, que acrescentou alguns tipos ao Código Penal Brasileiro, abaixo descritos:

Art. 313-A: Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano:

Pena- reclusão, de 2 (dois) a 12 (doze) anos, e multa.

Art. 313-B: Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente:

Pena- detenção, de 3 (três) meses a 2 (dois) anos, e multa.

Para a discussão do tema em questão, foi utilizado o método Bibliográfico, por meio de estudos de monografias, doutrinas, artigos científicos e livros especializados.

2.0 DIREITO E INFORMÁTICA

O crescente desenvolvimento tecnológico e alcance global da Internet chamou a atenção do Direito. É sabido que o objetivo do Direito é regular a vida em sociedade, estabelecendo para esse fim, normas de condutas, que devem ser seguidas por todos.

No mundo virtual não seria diferente. Para analisar as relações sociais e aspectos jurídicos que envolvem o uso do computador e as tecnologias de informação, nasceu o Direito da Informática. Esse novo campo do Direito, que é resultado da relação entre a ciência do Direito e a ciência das novas tecnologias, busca solucionar os inúmeros e complexos problemas que a esfera digital provoca.

Segundo Carlos Alberto Braz de Melo⁴,

A era digital caracteriza-se pela introdução de um novo conceito de espaço- o ciberespaço, e pela efetiva utilização de uma nova ferramenta: a Internet. Esta, por seu turno, tem se mostrado uma das principais armas da globalização, que afeta o mundo inteiro, ocasionando fatos e consequências jurídicas. (...) nesse novo ambiente surgem também inúmeros conflitos que a Ciência do Direito ainda não encontrou respostas e por isso apresenta-se um descompasso entre as inovações tecnológicas e a aplicação da ordem jurídica às mesmas.

⁴Disponível em: www.direitodainformatica.blogspot.com.br

Constata-se, portanto, que a rede de informática gera efeitos ainda não delimitados pelo Direito, principalmente pelo fato desta rede ser um local onde tempo, lugar, espaço e matéria não se refletem no mundo real de maneira tão simples. Esses elementos, no âmbito virtual, não são facilmente definidos.

Assim destaca Murilo Miranda⁵

O grande problema jurídico dessa modalidade de crime está situado nas esferas da jurisdição e competência, visto que o desenrolar na infração pode iniciar em um local, a consumação ocorrer em outro e o resultado em um terceiro diferente dos anteriores. Daí uma grande discussão quanto à teoria aplicável para fixar a competência. Seria a teoria da atividade a mais adequada? Fixando sua competência a partir do local de origem do crime? Ou poderia-se utilizar a teoria do resultado, deixando o processamento de tais demandas a cargo do local (ou locais) onde ocorreram os danos? Há também quem defenda a fusão das duas, a teoria da ubiquidade e sua fixação pela prevenção. Ainda assim, deve-se lembrar de que a Internet é global, o que pode estender o dano pelas mais remotas áreas do globo, a chamada transnacionalidade do dano.

A rede digital não tem limitação geográfica. A cada país, a cada Estado, cabe o dever de estabelecer sua jurisdição a fim de regularizar a criminalidade informática.

Pode-se dizer que a jurisdição é⁶:

Uma das funções do Estado, mediante a qual este se substitui aos titulares dos interesses em conflito para, imparcialmente, buscar a pacificação do conflito que os envolve, com justiça. Essa pacificação é feita mediante a atuação da vontade do direito objetivo que rege o caso apresentado em concreto para ser solucionado; e o estado desempenha essa função sempre mediante o processo, seja expressando imperativamente o preceito (através de uma sentença de mérito), seja realizando no mundo das coisas o que o preceito estabelece (através da execução forçada).

O Direito, assim, enfrenta um grande desafio. Ele precisa acompanhar a nova realidade e criar regras necessárias para lidar com os resultados que a era cibernética produz no universo jurídico, pois elas diferem do mundo físico.

⁵ MIRANDA, Murilo. **Da Persecução Penal dos Crimes Virtuais**. Disponível em http://www.jurisway.org.br/monografias/monografia.asp?id_dh=9903. Acesso em 15 de outubro de 2013

⁶ MIRABETE, Júlio Fabbrini. **Processo Penal**. 18. Rd. São Paulo: Atlas, 2008. P. 151.

O momento atual clama por uma dinâmica entre os países para discutir uma específica regulamentação e repressão aos ilícitos virtuais.

3.0 CONCEITO E CLASSIFICAÇÃO DOS CRIMES DE INFORMÁTICA

3.1. Conceito

Os delitos de informática tem chamado a atenção de doutrinadores, o que faz surgir inúmeras terminologias: crimes de computador, crimes digitais, crimes virtuais, crimes tecnológicos, crimes via Internet etc.. Mas a denominação crimes de informática adequa-se mais, visto que abrange todo o sistema informático. Além de termos, temos bastantes divergências condizentes ao conceito. Vários autores chegaram a uma definição.

Para João Marcello de Araújo Júnior,

Crime de informática é 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.⁷

Segundo Sérgio Marcos Roque (2000, p.309), “É a conduta definida em lei como crime em que o computador tiver sido utilizado como instrumento para a sua perpetração ou consistir em seu objeto material”.

Já Corrêa (2000, p.43) aduz que:

Crimes digitais seriam todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar; para tal prática é indispensável a utilização de um meio eletrônico.

Na visão de Carla Rodrigues Araújo Castro (2001, p.10):

Aquele praticado contra o sistema de informática ou através deste, compreendendo os crimes praticados contra o computador e seus acessórios e os perpetrados através do computador.

⁷ Computer Crime, in Anais da Conferencia Internacional de Direito Penal, 1988. Rio de Janeiro: PGDF, 1988, p.461.

Desse modo, percebe-se que não há um conceito uniforme sobre o tema. Logo, a definição ampla é mais coerente, pois os ilícitos penais virtuais envolvem todo o sistema informático, onde o computador é objeto ou instrumento do crime.

3.2. Classificação

Assim como no conceito, nota-se uma falta de consenso entre os autores no que diz respeito à classificação dos crimes de informática.

Para Ivette Senise Ferreira, os crimes virtuais consistem em:

Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro dele incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial.⁸

Antônio Scarance Fernandes (1999, p. 17-18) classifica tais crimes em:

- a) Crime de Informática Puro: o sistema informático é utilizado como meio e também como fim desejado pelo autor do crime;
- b) Crime de Informática Impuro: aqueles em que o agente não visa o sistema, mas a informática é instrumento indispensável para a consumação do crime;
- c) Crime de Informática Comum: aquele em que o agente não visa o sistema, mas usa a informática como instrumento (não essencial) de realização da conduta criminosa.

Dentre todas as classificações existentes, a dividida entre crimes virtuais próprios e impróprios é a mais adotada.

3.2.1. Crimes virtuais próprios

São os crimes em que a informática é necessária para poderem ser praticados, sem ela a execução do delito torna-se impossível. Estes são delitos

⁸Os Crimes de Informática, Estudos Jurídicos em Homenagem a Manoel Pedro Pimentel, pp. 146-154.

que causam maiores problemas para os operadores do direito, pois são os crimes novos, que nasceram junto com a evolução tecnológica e afetam a informática como bem juridicamente protegido. Sendo assim, não possuindo legislação específica, alguns fatos são atípicos e, portanto inimputáveis.

São exemplos, invasão de dados, envio de vírus, violação de e-mail, pirataria de software e etc.

3.2.2. Crimes virtuais impróprios

São os crimes que podem ser praticados de qualquer forma, com ou sem a utilização do sistema de informática, logo a rede de computador não é essencial para a execução e consumação do delito, e que atinge todo o bem jurídico já tutelado. Ou seja, crimes já tipificados, logo são punidos adequadamente de acordo com a legislação comum, mas que agora podem ser praticados através do computador.

São exemplos, a pedofilia, calúnia, estelionato, furto e etc.

4.0. SUJEITOS NOS CRIMES DE INFORMÁTICA

O Crime de Informática é comum quanto ao agente, ou seja, qualquer pessoa pode ser sujeito do delito, ativo ou passivo, basta estar em um computador conectado à Internet.

4.1. Sujeito ativo

Rol dos criminosos virtuais⁹:

HACKER – este indivíduo em geral domina a informática, é muito inteligente, adora invadir sites, mas na maioria das vezes não com a finalidade de cometer crimes, costumam se desafiar entre si, para ver quem consegue invadir tal sistema ou página na Internet, isto apenas para mostrar como estamos vulneráveis no mundo virtual. Várias empresas estão contratando há

⁹ NOGUEIRA, Sandro D'Amato, **Crimes de Informática**. São Paulo: BH Editora, 2009. p 69-70.

tempos os Hacker's para proteção dos seus sistemas, banco de dados, seus segredos profissionais, fraudes eletrônicas, etc.

CRACKER – são os verdadeiros criminosos. Usam a Internet para cometer crimes, fraudes bancárias e eletrônicas, furto de dados, golpes e grandes estragos. São verdadeiras quadrilhas de jovens que não se contentam apenas em invadir um sistema, usam sua inteligência e domínio da informática para causar prejuízos de milhares de reais, tanto contra pessoas físicas, como jurídicas, órgãos públicos, etc.

PHREAKERS – este é o “terror das companhias telefônicas”. São criminosos especializados em burlar sistemas de telefonia. Os prejuízos são enormes e incalculáveis.

Fabrício Rosa¹⁰ define *phreaker* como sendo

Aquele especializado em telefonia. Atua na obtenção de ligações telefônicas gratuitas e instalação de escutas, facilitando o ataque a sistemas a partir de acesso exterior, tornando-se invisíveis ao rastreamento ou colocando a responsabilidade em terceiro;

DEFACERS (PICHADORES VIRTUAIS) – estes adoram invadir algum site e desfigurar a página, a maioria do poder público, como FBI, Pentágono, STF, INSS, e lá deixar sua marca. Normalmente não causam danos. O autor só poderá ser incriminado caso gere algum prejuízo patrimonial ao dono do site.

SPAMMERS- são pessoas e empresas que enviam e-mails indesejados, muitas vezes lotando sua caixa de e-mails com pornografia, propaganda, lançamento de produtos, etc.

CYBER TERRORISTA – fazem apologia ao terrorismo e ataques em massa, postam vídeos com mensagens de ódio e orientações de ataques a inimigos, estes muitas vezes com o cunho religioso.

4.1.2 Outros sujeitos

Vale salientar que os crimes virtuais não são necessariamente praticados apenas por pessoas com vasto conhecimento na área da

¹⁰ ROSA, Fabrício. **Crimes de Informática**. 2.ed. Campinas: BookSeller, 2006. P. 62.

computação. Usuários comuns também podem cometer esses delitos, basta saber usar o computador e a Internet.

4.2. Sujeito passivo

É a vítima, o que sofre a ação do sujeito ativo. Pode ser qualquer indivíduo normal, pessoa física, ou até mesmo uma pessoa jurídica que utiliza um computador ou qualquer outra tecnologia informática (caixa eletrônico, smartphone etc.). Assim afirma Sandro D'Amato Nogueira¹¹: "qualquer um de nós pode ser vítima, todos nós que temos acesso a rede mundial de computadores estamos arriscados a sermos vítimas dos delitos informáticos".

O sujeito passivo, na maioria das vezes, prefere não tornar público o fato de ter sido lesado por um criminoso virtual, o que prejudica a punição do delito, visto que as autoridades competentes não tomarão conhecimento do crime.

5.0. O DIREITO PENAL BRASILEIRO E OS CRIMES DE INFORMÁTICA

5.1. Princípio da legalidade e tipicidade penal

Seja dentro ou fora do mundo virtual, sabe-se que é através da lei que se previne e pune a ação de criminosos. Ela é responsável por determinar as condutas do homem frente aos princípios sociais. Logo, a lei é essencial. É sabido, também, que, devido ao princípio da legalidade, conhecido também como princípio da reserva legal, prevalente na Constituição Brasileira¹² e ratificado na legislação infraconstitucional, disposto no Código Penal Brasileiro, não pode ser considerado crime, conduta que não esteja prevista em lei.

Com precisão, explica Marco Antônio Marques da Silva que:

O princípio da legalidade ou reserva legal constitui um efetivo limite ao poder punitivo do Estado e, na medida em que impede a criação de tipos penais, a não ser de processo legislativo regular, se caracteriza por ser, também um limite ao poder normativo do Estado.¹³

¹¹ NOGUEIRA, Sandro D'Amato, **Crimes de Informática**. São Paulo: BH Editora, 2009.p 75.

¹² CF/88, art. 5º, XXXIX: "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal".

¹³ Marco Antônio Marques da Silva. **Acesso à Justiça Penal e Estado Democrático de Direito**. São Paulo, Ed. J. de Oliveira, 2001, p. 07.

No entendimento de Fernando Capez, referente ao princípio da legalidade:

Somente haverá crime quando existir a perfeita correspondência entre a conduta praticada e a previsão legal, as normas penais incriminadoras não são proibitivas, mas descritivas; portanto quem pratica um crime não contra a lei, mas sim de acordo com esta, pois os delitos encontram-se pormenorizadamente descritos nos modelos legais, chamados de tipos. Cabe, portanto, a lei a tarefa de definir e não proibir o crime, propiciando ao agente prévio e integral conhecimento das consequências penais da prática delituosa e evitando, assim, qualquer invasão arbitrária ao seu direito de liberdade.¹⁴

O princípio da legalidade constitui o princípio penal básico, e é ele quem ampara a tipicidade penal. Para Mirabete: “Tipicidade é a correspondência exata, a adequação perfeita entre o fato natural concreto e a descrição contida em lei.”¹⁵

A realidade é que muitos crimes de informática não possuem tipificação específica nas leis brasileiras. Diversas modalidades de delitos praticados por meio da internet não podem ser passíveis de punição.

Carla Rodrigues Araújo de Castro¹⁶ elucida sobre a falta de legislação referente aos crimes virtuais:

Nos crimes praticados através da informática, ou seja, tipos antigos, nos quais o agente utiliza a informática como meio de execução, como instrumento da sua empreitada, não há dificuldades, o crime é mesmo previsto em sua origem, a forma de sua execução é que inovou, por exemplo, uma ameaça feita pessoalmente não se distingue na tipicidade de uma ameaça virtual.

Problema surge em relação aos crimes cometidos contra o sistema de informática, atingindo bens não tutelados pelo legislador, como dados, informações, *hardware*, sites, *home pages*, e-mail etc.. São condutas novas que se desenvolveram junto com nossa sociedade razão pela qual o legislador de 1940, época do Código Penal, não pôde prever tais tipos penais.

Nessas situações é comum os Tribunais tentarem adequar crimes sem tipificação aos já descritos em lei, por meio de analogia. Porém, o princípio da

¹⁴CAPEZ, Fernando. **Curso de Direito Penal, volume 1: parte geral**. São Paulo. Saraiva, 2010 p.59.

¹⁵MIRABETE, Julio Fabbrini, **Manual do Direito Penal, volume 1: parte geral**. Julio Fabbrini Mirabete, Renato N. Fabbrini -24 ed São Paulo: Atlas, 2008 p.110.

¹⁶CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. 2. Ed. Rio de Janeiro, Lumem Juris, 2003. P.217.

reserva legal não admite interpretação analógica, salvo se for para beneficiar o réu. Assim explica Fernando Capez:

A aplicação da analogia em norma penal incriminadora fere o princípio da reserva legal, uma vez que um fato definido em lei como crime, estaria sendo considerado como tal. Imagine considerar típico o furto de uso (subtração de coisa alheia móvel para o uso), por força da aplicação da analogia do artigo 155 do Código Penal (subtrair coisa alheia móvel com ânimo de assenhoramento definitivo). Neste caso, um fato não considerado criminoso pela lei passaria a sê-lo, em evidente afronta ao princípio do art. 5º, XXXIX (reserva legal). A analogia *in malam partem*, em princípio, seria impossível, pois jamais seria benéfica ao acusado a incriminação de um fato atípico.¹⁷

Faz-se, portanto, imprescindível a criação de uma legislação específica capaz de conduzir os crimes de informática para que a impunidade no âmbito virtual tenha um fim.

5.2. Lugar do crime: princípio da territorialidade

Uma das maiores dificuldades para se combater os crimes virtuais diz respeito à territorialidade. A Internet, por ser globalizada, possibilita que um ato ilícito seja praticado em qualquer lugar do mundo, sem que o agente sequer tenha saído de sua residência.

Os delitos realizados por intermédio de tecnologia informática podem atingir mais de uma pessoa, em diferentes localidades, com legislações distintas. Desse modo, é necessário determinar o lugar do crime, para que seja verificada a adoção ou não da lei pátria.

A aplicação da legislação brasileira segue o disposto no artigo 5º do Código Penal.

Dispõe o artigo 5º do Código Penal Brasileiro, no tocante à territorialidade¹⁸:

Art. 5º - Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional.

§ 1º - Para os efeitos penais, consideram-se como extensão do território nacional as embarcações e aeronaves brasileiras, de natureza pública ou a serviço do governo brasileiro onde quer que se encontrem, bem como as

¹⁷ CAPEZ, Fernando. **Curso de Direito Penal, volume 1: parte geral**. São Paulo. Saraiva, 2010 p.59.

¹⁸ BRASIL. Decreto-Lei nº 2.848 de 7 de dezembro de 1940. Código Penal.

aeronaves e as embarcações brasileiras, mercantes ou de propriedade privada, que se achem, respectivamente, no espaço aéreo correspondente ou em alto-mar.

§ 2º - É também aplicável a lei brasileira aos crimes praticados a bordo de aeronaves ou embarcações estrangeiras de propriedade privada, achando-se aquelas em pouso no território nacional ou em vôo no espaço aéreo correspondente, e estas em porto ou mar territorial do Brasil.

Entretanto, o Brasil adota em seu art. 6º do Código Penal, utilizado para solucionar os problemas relativos aos delitos informáticos, a teoria da ubiquidade: “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 devia produzir o resultado”. Onde afirma ser lugar do crime tanto o do ato da execução (ação ou omissão total ou parcial), quanto o do resultado (efetivo ou tentado).

Portanto, para que a lei brasileira seja aplicada, basta que o crime toque o território nacional, seja de maneira direta ou indireta. A maneira direta seria a execução e o resultado do crime dentro do Brasil. A maneira indireta seria a execução do crime fora do país, mas com resultado no Brasil ou vice e versa.

Para esclarecer a teoria em questão, o doutrinador Damásio de Jesus (2003, p.129), cita um exemplo: “na fronteira Brasil-Bolívia um cidadão brasileiro, que se encontra em território nacional, atira em outro, em solo boliviano, vindo este a falecer”. Pela teoria da ubiquidade, considera-se praticado o crime tanto no Brasil quanto na Bolívia.

Toma-se como exemplo, também, um indivíduo X que envia um e-mail da Europa para o indivíduo Z em Natal contendo vírus e danificando todos os arquivos, a lei brasileira será utilizada.

O artigo 7º, inciso II, alínea “a”, do Código Penal¹⁹ versa sobre os casos especiais de extraterritorialidade, tendo como base os princípios da justiça universal, nacionalidade e personalidade. Assim dispõe:

Art. 7º - Ficam sujeitos à lei brasileira, embora cometidos no estrangeiro:

II - os crimes:

a) que, por tratado ou convenção, o Brasil se obrigou a reprimir;

¹⁹ BRASIL. Decreto-Lei nº 2.848 de 7 de dezembro de 1940. Código Penal

Diante do exposto, é notório que a legislação brasileira terá aplicabilidade quando a ação criminosa, parte dela ou as consequências ocorrerem no Brasil. Logo, mesmo que processado e punido em país diverso, o agente será julgado perante as leis nacionais.

Independente de qual norma deverá ser imposta, para que os delitos virtuais sejam combatidos é imprescindível a cooperação entre estados e países para que as leis sejam utilizadas de forma satisfatória e eficiente. Frente ao alcance internacional que a internet é capaz de atingir, Maria Eugenia Finkelstein²⁰ acredita ser importante a uniformização das leis por todos os países:

O caráter global da internet e a possibilidade de crimes informáticos internacionais são pontos que devem ser considerados. Em face desse caráter, qualquer mudança legislativa deveria ser implementada por vários países no sentido de uniformizar as leis por meio de esforços internacionais no sentido de harmonizar as práticas. O maior erro que poderíamos cometer seria o de tentar resolver os problemas gerados pela internet pensando individual e regionalmente, sem a inserção no contexto internacional. Afinal, a internet não é um assunto de âmbito meramente local, mas, sim, global.

5.3 Conflitos de Competência: Jurisprudência

Para evidenciar a questão do lugar do crime, elencada acima, e a definição da competência para julgar o delito, segue jurisprudência²¹ relativa ao crime de Pedofilia praticada via Internet:

Processo:	RSE 102383520134013500 GO 0010238-35.2013.4.01.3500
Relator(a):	DESEMBARGADORA FEDERAL MONICA SIFUENTES
Julgamento:	23/07/2013
Órgão Julgador:	TERCEIRA TURMA
Publicação:	e-DJF1 p.106 de 02/08/2013

²⁰ FINKELSTEIN, Maria Eugenia. Fraude Eletrônica.

²¹ Recurso em Sentido Estrito. Disponível em <http://trf1.jusbrasil.com.br/jurisprudencia/23885068/recurso-em-sentido-estrito-rse-102383520134013500-go-0010238-3520134013500-trf1>. Acesso

em 07 de novembro de 2013

Ementa

PENAL E PROCESSUAL PENAL. CRIME DE PEDOFILIA (ART. 241, LEI 8.069/90). DIVULGAÇÃO DE IMAGENS PELA REDE MUNDIAL DE COMPUTADORES. COMPETÊNCIA DA JUSTIÇA FEDERAL. RECURSO PROVIDO.

1. Recurso em sentido estrito contra decisão que reconheceu a incompetência da Justiça Federal acerca da suposta prática do crime previsto no art. 241-A da Lei 8.069/90, no sítio de relacionamento orkut.

2. O Brasil é signatário da "Convenção sobre Direito da Criança", incorporada ao direito pátrio mediante o Decreto Legislativo n. 28/90 e promulgada pelo Decreto Presidencial n. 99.710/90, bem como do "Protocolo Facultativo à Convenção sobre os Direitos da Criança referente à venda de criança, prostituição infantil e à pornografia infantil", aprovada pelo Congresso Nacional através do Decreto Legislativo n. 230, de 29/05/2003, com texto publicado em 08/03/2004, por meio do Decreto Executivo n. 5.007/2004, no qual se registrou a preocupação "com a crescente disponibilidade de pornografia infantil na internet e em outras tecnologias modernas".

3. Em que pese o fato de os arquivos com conteúdo pornográfico infantil terem sido disponibilizados em território nacional, basta a mera possibilidade desse acesso, via rede mundial de computadores para que se configure a competência da Justiça Federal, conforme previsão contida no art. 109, inciso V da Constituição Federal.

4. Tratando-se de divulgação de imagens pornográficas, envolvendo crianças e adolescentes, por meio do orkut - comunicação eletrônica disponibilizada para qualquer indivíduo, inclusive fora do Brasil - verifica-se a ocorrência da transnacionalidade a atrair a competência da Justiça Federal.

5. Compete à Justiça Federal processar e julgar o feito, eis que trata do cometimento de delito por meio eletrônico que se refere às infrações previstas em tratados ou convenções internacionais, cujo acesso se dá além das fronteiras do território nacional. 5. Recurso provido para reconhecer a competência da 5ª Vara Federal da Seção Judiciária de Goiás.

Acórdão

A Turma, por unanimidade, deu provimento ao recurso em sentido estrito.

[...] Narra a denúncia que em 02/05/2011 o usuário do perfil "gago_lokao@hotmail.com" ameaçou e constrangeu a menor Letícia Vilar, nascida em 14/09/1997 e residente em Curitiba/PR, a exibir partes íntimas de seu corpo diante de *webcam*, imagens que foram posteriormente postadas em perfil virtual da vítima no *orkut*. Após as investigações constatou-se que as conexões à *internet* partiram da cidade de Piranhas/GO.

O Juiz Federal da 5ª Vara da Seção Judiciária de Goiás, Alderico Rocha Santos, declinou a competência, em relação à apuração de suposta prática do crime do art. 241-A da Lei 8.069/90, para processar e julgar o presente feito, à Justiça Estadual, sob o fundamento de que a denúncia não aponta

nenhum dado concreto no sentido de que as imagens disponíveis na *internet* tenham sido visualizadas no exterior determinando a remessa dos autos ao Juiz de Direito da Comarca de Piranhas/GO.

O Ministério Público Federal apresentou suas razões de recurso; requerendo, em resumo, que fosse mantida a competência da Justiça Federal, sob o argumento de que a pornografia infantil foi objeto da convenção da Organizações das Nações Unidas sobre direitos da criança, da qual o Brasil é signatário, e que foi incorporada ao direito pátrio.

Alega que a inserção de imagens pedopornográficas (crianças/adolescentes), em rede internacional, permite a publicação instantânea - seja no Brasil, seja no exterior - o que dá lugar à competência da Justiça Federal.

Dispõe o art. 109, inciso V, da Constituição Federal:

Art. 109. Aos juízes federais compete processar e julgar:

(...)

v - os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente.

No caso, em que pese o fato de os arquivos com conteúdo pornográfico infantil terem sido disponibilizados em território nacional, basta a mera possibilidade desse acesso via rede mundial de computadores para que se configure a competência da Justiça Federal, conforme previsão contida no artigo citado.

Nessa linha de raciocínio é o posicionamento adotado por esta Corte, como se pode ver no seguinte precedente:

PROCESSUAL PENAL - CRIME PREVISTO NO ART. 241-A, CAPUT, DA LEI 8.069/90 (REDAÇÃO DA LEI 11.829/2008) - CONVENÇÃO SOBRE OS DIREITOS DA CRIANÇA, SUBSCRITA PELO BRASIL - TRANSNACIONALIDADE DO CRIME DE INSERÇÃO DE FOTOGRAFIAS PORNOGRÁFICAS DE CRIANÇAS, NA REDE INTERNACIONAL DE COMPUTADORES (INTERNET) - COMPETÊNCIA DA JUSTIÇA FEDERAL - ART. 109, V, DA CF/88 - PRECEDENTES DO STF, DO STJ E DO TRF/1ª REGIÃO - RECURSO PROVIDO.

I - O art. 109, V, da CF, estabelece que compete aos juízes federais processar e julgar "os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente".

II - A competência para processar e julgar o crime previsto no art. 241-A, caput, da Lei 8.069, de 13/07/1990, na redação da Lei 11.829/2008, é da Justiça Federal, por ser o Brasil signatário da Convenção sobre os Direitos da Criança, promulgada pelo Decreto nº 99.710, de 21/11/1990, desde que presente a transnacionalidade do delito.

III - Hipótese de publicação, na página de relacionamento do ORKUT, na rede mundial de computadores (Internet), de

imagens com cenas envolvendo pornografia infantil (art. 241-A, caput, da Lei 8.069, de 13/07/1990, na redação da Lei 11.829/2008).

IV - Ao apreciar espécie análoga, a jurisprudência do colendo STF, do egrégio STJ e do TRF/1ª Região orienta-se no sentido de fixar a competência da Justiça Federal, na forma do art. 109, V, da CF/88, ao fundamento de que, além de o Brasil ser signatário de tratado ou convenção internacional que prevê o combate a atividades criminais dessa natureza, o crime se consuma com a publicação, na rede mundial de computadores (Internet), de fotografias de pornografia infantil, dando o agente causa ao resultado da publicação, legalmente vedada, dentro e fora dos limites do território nacional (STF, HC 86289/GO, Rel. Min. Ricardo Lewandowski; STJ, CC 29.886/SP, Rel. Min. Maria Thereza de Assis Moura; STJ, CC 111.338/TO, Rel. Min. Og Fernandes; TRF/1ª Região, RSE 2007.38.00.025788-1/MG, Rel. Des. Federal Tourinho Neto).

V - "No presente caso, há hipótese de atração da competência da Justiça Federal, uma vez que o fato de haver um usuário do Orkut, supostamente praticando delitos de divulgação de imagens pornográficas de crianças e adolescentes, configura uma das situações previstas pelo art. 109 da Constituição Federal. Além do mais, é importante ressaltar que a divulgação de imagens pornográficas, envolvendo crianças e adolescentes por meio do Orkut, provavelmente não se restringiu a uma comunicação eletrônica entre pessoas residentes no Brasil, uma vez que qualquer pessoa, em qualquer lugar do mundo, desde que conectada à internet e pertencente ao dito sítio de relacionamento, poderá acessar a página publicada com tais conteúdos pedófilos-pornográficos, verificando-se, portanto, cumprido o requisito da transnacionalidade exigido para atrair a competência da Justiça Federal." (STJ, CC 111.338/TO, Rel. Min. OG FERNANDES, 3ª Seção, unânime, julgado em 23/06/2010, DJe de 01/07/2010).

VI - "Diante de existência de tratado ou convenção internacional que prevê o combate à prática de atividades criminosas, envolvendo menores, e, sendo o Brasil signatário da Convenção sobre os Direitos da Criança, a competência para processar e julgar o feito é da Justiça Federal. A inserção de fotos pornográficas de crianças na rede internacional permite a publicação instantânea, seja no Brasil seja no exterior, o que dá lugar à competência da Justiça Federal". (TRF/1ª Região, RSE 2007.38.00.025788-1/MG, Rel. Des. Federal Tourinho Neto, 3ª Turma, unânime, e-DJF1 de 19/12/2008, p. 395)

VII - A transnacionalidade de tais delitos, cometidos pela Internet, é inerente ao próprio ambiente da rede mundial de computadores, que permite o acesso de qualquer pessoa à página do ORKUT, em qualquer lugar do mundo, desde que conectada à Internet e pertencente à referida rede social.

VIII - Recurso provido, para reconhecer a competência da Justiça Federal. (RSE 0004578-55.2011.4.01.0000 / GO, Rel. DESEMBARGADORA FEDERAL ASSUSETE MAGALHÃES, TERCEIRA TURMA, e-DJF1 p.186 de 08/04/2011).

Portanto, compete à Justiça Federal processar e julgar o feito, eis que trata do cometimento de delito por meio eletrônico que se refere às infrações previstas em tratados ou convenções internacionais, cujo acesso se dá além das fronteiras do território nacional.

5.4. O problema da autoria

Identificar a autoria dos crimes virtuais é um processo bastante complicado. Essa dificuldade não atinge apenas o Brasil, mas todos os países que se deparam com esse tipo de delito.

Presumindo, por exemplo, que uma vítima do cyber crime, que tenha seu computador danificado por um vírus recebido, vá a uma Delegacia de Polícia dar ocorrência do fato (o que raramente acontece). A partir da notificação do sujeito passivo é que se inicia a dificuldade, pois se o país carece de tecnologia, as autoridades sequer saberão de onde partiu o e-mail contendo vírus.

Diferente do “mundo real”, a identificação do autor no ciberespaço não pode ser visual.

Quando um sujeito está on-line na rede, há apenas dois elementos identificadores: o endereço do computador que deu origem às informações criminosas e o endereço na máquina que recebe os dados. Tais endereços são denominados IP – *Internet Protocol*. O IP, de forma genérica, é uma identificação de um dispositivo (computador, impressora, etc.) em uma rede local ou pública. Cada computador na internet possui um IP único.²² O IP tem 11 dígitos e no Brasil começa sempre com 200 ou 201.

Porém, isso não é suficiente para solucionar o problema. As pessoas que praticam ilícitos desse gênero, na grande maioria das vezes, possuem um vasto domínio da informática e, portanto, conseguem agir sem deixar vestígios ou suspeitas.

²² Endereço IP. pt.wikipedia.org/wig/endereço.ip

A título de exemplo, os *hackers* costumam utilizar celulares clonados para ter acesso à internet, inviabilizando a identificação do local da chamada e de seu autor (Vladimir Aras, 2002).

De acordo com Vladimir Aras²³:

O único método realmente seguro de atribuição de autoria em crimes informáticos é o que se funda no exame de atuação do responsável penal, quando este se tenha valido de elementos corporais para obter acesso a redes ou computadores. Há mecanismos que somente validam acesso mediante a verificação de dados biométricos do indivíduo. Sem isso a entrada no sistema é vedada. As formas mais comuns são a análise do fundo do olho do usuário ou a leitura eletrônica de impressão digital, ou ainda, a análise de voz do usuário [...]. Como dito, somente os mecanismos de assinatura eletrônica, certificação digital e de análise biométrica podem conferir algum grau de certeza quanto à autoria da mensagem, da informação, ou da transmissão, se considerado o problema no prisma penal.

Como se vê, a solução existe, mas não é simples. O Brasil não possui os meios necessários para empregá-las. Entretanto, nada é impossível. Deve-se acreditar que os operadores do Direito estão caminhando para sanar os incontestáveis problemas.

5.5. Projetos de lei em tramitação no Congresso Nacional

Há diversos projetos de lei em tramitação no Congresso Nacional pertinentes aos crimes cibernéticos, com o propósito de veicular novos tipos penais. Dentre eles, destacam-se o Projeto nº 84/1999, do Deputado Luiz Piauhyllino (já aprovado na Câmara dos Deputados e em tramitação no Senado Federal como o PLC nº 89/2003), e o Projeto nº 76/2000, do Senador Renan Calheiros.

Nota-se, pelas datas, que as propostas aguardam aprovação há anos.

O PLS nº 76, de 2000, de autoria do Senador Renan Calheiros, apresenta tipificação de condutas praticadas com o uso de computadores, e lhes atribui as respectivas penas, sem alterar, entretanto, o Código Penal.

Classifica os crimes cibernéticos em sete categorias: contra a inviolabilidade de dados e sua comunicação; contra a propriedade e o

²³ ARAS, Vladimir. Crimes de Informática. Uma nova criminalidade. Jus Navigandi, n.51. [internet]. Disponível em: <http://jus2.uol.com.br/doutrina/texto.aspx?id=2250>. Acesso em 28 de out. 2013.

patrimônio; contra a honra e a vida privada; contra a vida e a integridade física das pessoas; contra o patrimônio fiscal; contra a moral pública e a opção sexual; e contra a segurança nacional.

O PLC nº 89, de 2003, de iniciativa do Deputado Luiz Piauhyllino, altera o Decreto lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), e a Lei nº 9.296, de 24 de julho de 1996, e dá outras providências.²⁴

Dentre as alterações que este projeto de lei trará a legislação, podem-se citar algumas²⁵:

- a) O art. 2º prevê a inclusão do Capítulo IV do Título VIII, da Parte Especial do Código Penal, com a redação dos arts. 285-A (acesso não autorizado a sistemas informáticos), 285-B (obtenção e transferência ilegal de dados) e 285-c (ação penal);
- b) O art. 3º prevê a inclusão do art. 154-A no Título I, Capítulo VI, Seção IV, que trata da divulgação ou utilização indevida de informações e dados pessoais;
- c) O art. 4º trata da alteração do art. 163, inserido no Título II, Capítulo IV, para que inclua no crime de dano a destruição, inutilização ou deterioração de dados alheios.
- d) O art. 5º trata ta inclusão do art. 163-A, no mesmo Título II, Capítulo IV, que incrimina a disseminação de vírus computacional;
- e) O art. 6º altera o crime de estelionato para que conste no art. 171, § 2º, VII, a difusão de vírus que vise destruir, copiar, alterar, facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado, para obter vantagem econômica para si ou para outrem, em detrimento de outrem;
- f) O art. 7º altera os crimes dos arts. 265 e 266 do CP para que constem como crime contra a segurança de serviços de utilidade pública os de informação e telecomunicações;
- g) O art. 8º altera o art. 297 do CP para que dentre as falsificações de documentos públicos incluam-se os dados;
- h) O art. 9º altera o art. 298 do CP para que dentre as falsificações de documentos particulares incluam-se os dados;
- i) O art. 10 muda o Código Penal Militar para que o art. 251 do Capítulo IV, do Título V da Parte Especial do Livro I do Decreto-Lei n. 1001, de 21 de outubro de

²⁴ NOGUEIRA, Sandro D`Amato, **Crimes de Informática**. São Paulo: BH Editora, 2009, p 205.

²⁵ CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo. Saraiva, 2001. P. 164 a 169.

- 1969 (Código Penal Militar), passe a vigorar acrescido do inciso VI ao seu § 1º, e do § 4º, incriminando-se o estelionato eletrônico;
- j) O art. 11 altera o *caput* do art. 259 e o *caput* do art. 262 do Capítulo VII, do Título V, da Parte Especial do Livro I do Decreto-Lei n. 1001, de 21 de outubro de 1969 (Código Penal Militar), para que deles conste destruição a dados sob administração militar;
 - k) O art. 12 altera o Capítulo VII, do Título V, da Parte Especial do Livro I do Decreto-Lei n. 1001, de 21 de outubro de 1969 (Código Penal Militar), que fica acrescido do art. 262-A, prevendo a disseminação de vírus em sistemas militares;
 - l) O art. 13 altera o Capítulo VII, do Título V, da Parte Especial do Livro I do Decreto-Lei n. 1001, de 21 de outubro de 1969 (Código Penal Militar), que fica acrescido do Capítulo VII-A, que prevê crimes contra a segurança dos sistemas informatizados;
 - m) O art. 14 altera o *caput* do art. 311 do Capítulo V, do Título VII, da Parte Especial do Livro I do Decreto-Lei n. 1001, de 21 de outubro de 1969 (Código Penal Militar), para que a falsificação dos documentos inclua os dados;
 - n) O art. 15 altera os incisos II e III do art. 356, do Capítulo I, do Título I, do Livro II da Parte Especial do Decreto-Lei n. 1001, de 21 de outubro de 1969 (Código Penal Militar), para que conste do crime de favorecer o inimigo a entrega de dados;
 - o) O art. 16 traz definições do que devem ser considerados dispositivo de comunicação, sistema informatizado, rede de computadores, código malicioso, dados informáticos e dados de tráfego;

Com a devida aprovação desses projetos de leis, o dilema da tipificação dos delitos de informática tende a melhorar.

5.6. Lei 12.737/12 – “Lei Carolina Dieckmann”

Além desses projetos em tramitação, foi publicada no Diário Oficial da União (DOU) a Lei nº 12.737 de 30 de novembro de 2012. Ela também dispõe acerca da tipificação dos crimes virtuais.

A lei, como primeira providência, origina o tipo penal *Invasão de dispositivo Informático* no art. 154-A do Código Penal com a seguinte redação:

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.

Para o advogado Auriney Brito:²⁶

O dia 03 de abril de 2013, data em que a lei entrou em vigor, ficou marcado na história pelo substancial avanço legislativo no que concerne à criminalidade informática. A Lei foi sancionada pela presidente Dilma Rouseff, com a dura missão de estreitar as já mencionadas lacunas existentes na matéria.

[...] A segurança informática, portanto, entendida como a *disponibilidade, confidencialidade e integridade* das informações dos usuários, há tempo já clamava por proteção jurídico-penal. Assim, com o advento da nova lei mencionada, os usuários das novas tecnologias de informação passam a ficar amparados pela lei, caso venham a sofrer ataques semelhantes ao que sofreu a atriz Carolina Dieckmann. Em que pese esse não ter sido o primeiro caso de extorsão e divulgação de conteúdo sigiloso na internet, foi o que deu maior repercussão midiática, que, sem dúvidas, é o fundamento da maior parte das ultimas criações legislativas do âmbito penal.

Idealizada pelo deputado Paulo Teixeira (PT-SP), a lei foi apelidada de “Lei Carolina Dickmann”, porque “o caso da atriz deu velocidade ao processo legislativo que deu ensejo à mudança”. Na época em que o projeto tramitava na Câmara de Deputados, a atriz teve fotos pessoais divulgadas sem autorização. Os *crackers* copiaram as fotos do seu computador e extorquiram a vítima para que não lançassem suas imagens na internet.

A nova lei classifica como crime justamente casos como esse, em que há a invasão de computadores, tablets ou smartphones conectados ou não à internet, “com o fim de obter, adulterar ou destruir dados ou informações”.²⁷

6.0 DOS CRIMES EM ESPÉCIE

²⁶ Análise da lei 12.12737/12- “Lei Carolina Dieckmann”. Disponível em <http://atualidadesdodireito.com.br/aurineybrito/2013/04/03/analise-da-lei-12-73712-lei-carolina-dieckmann/>. Acesso em 9 de novembro de 2013.

²⁷ “Lei Carolina Dieckmann” sobre crimes da internet entra em vigor. Disponível em <http://tecnologia.uol.com.br/noticias/redacao/2013/04/02/lei-carolina-dieckmann-sobre-crimes-na-internet-entra-em-vigor.htm>. Acesso em 8 de novembro de 2013.

São os delitos mais relevantes e constantes no contexto virtual, classificados neste artigo como “crimes virtuais impróprios”. São aqueles em que a informática não é necessária para a prática do delito, ela é apenas um meio. Desse modo, possuem previsão legal. A dificuldade de punir encontra-se apenas nas questões já discutidas, relativas à autoria e competência.

Segue tabela elaborada pela DRCI- Delegacia de Repressão aos Crimes de Informática - com as modalidades delituosas cometidas por meio da Internet e que já são previstas em lei:

Calúnia	Art. 138 do Código Penal (CP)
Difamação	Art. 139 do CP
Injúria	Art. 140 do CP
Ameaça	Art. 147 do CP
Furto	Art. 155 do CP
Dano	Art. 163 do CP
Apropriação Indébita	Art. 168 do CP
Estelionato	Art. 171 do CP
Violação ao Direito Autoral	Art. 184 do CP
Pedofilia	Art. 247 da Lei 8.069/90
Estatuto da Criança e do Adolescente	
Crime contra a Propriedade Industrial	Art. 183 e segs. da Lei 9.279/96
Interceptação de Comunicações de Informática	Art. 10 da Lei 9.296/96
Interceptação de e-mail comercial ou pessoal	Art. 10 da Lei 9.296/96
Crimes contra Software- “Pirataria”	Art. 12 da Lei 9.609/98

7.0. FATOS ATÍPICOS

No mundo virtual, existe a prática de condutas delituosas que, penalmente falando, são tidas como atípicas. Isso em decorrência da ausência de legislação específica concernente ao universo da informática.

Como já foi dito, essas condutas, em uma vez ou outra, podem se adequar às normas penais vigentes. Entretanto, essa solução por analogia não

é totalmente eficaz, servindo apenas para sanar as lacunas da lei, pois muitas vezes os agentes não são punidos.

A realidade é que os acusados não poderão ser acusados por condutas que não se enquadram em nenhum tipo penal.

Segue algumas condutas tidas ainda como atípicas, elencadas por Guilherme Guimarães ²⁸.

- *Spam* inábil à provocação de dano.
- Invasão, pela ação de *hackers*, de IP (Protocol Internet), sem prejuízo sensível.
- Alteração indevida, pela ação de *hackers*, de *web pages* mantidas por terceiros, sem prejuízo sensível.
- Violação, sonegação ou destruição de e-mail.
- Uso de nome alheio em domínio próprio para extorsão
- Interceptação ou escuta de fluxo de dados fora de tráfego típico de serviço de telecomunicações.

Além dessas, existem muitas outras ações delituosas as quais não cabe punição. E, se levarmos em consideração o incontestável fato de que as tecnologias de informação só tendem a evoluir, a propensão é que a situação se agrave. Portanto é imprescindível a criação de leis capazes de lidar com o problema de maneira mais apropriada e eficiente.

8.0. DIREITO COMPARADO

Diante de tudo que já foi elencado, é notória a carência de legislação no Brasil frente a era digital. Tendo destaque apenas alguns Projetos de Lei.

Diferente do nosso país, muitas nações já dispõem de leis específicas para tipificar os ilícitos virtuais, tratando não só de crimes, mas da informática e da Internet em geral.

²⁸FELICIANO, Guilherme Guimarães. **Informática e Criminalidade**: Primeiras Linhas. Ribeirão Preto: Nacional de Direito, 2001.

8.1 Convenção de Budapeste

Também conhecida como Convenção sobre o Cibercrime, a Convenção de Budapeste é um “tratado internacional de direito penal e processual firmado no âmbito do Conselho da Europa para definir de forma harmônica os crimes praticados por meio da Internet.”²⁹ Foi firmada em novembro de 2001, sem a participação do Brasil. Os Estados Unidos são o único país fora do Conselho da Europa que o ratificou.

A Convenção é um modelo de colaboração entre Estados para a luta contra os crimes virtuais. Seu preâmbulo constata isso³⁰:

Reconhecendo a necessidade de uma cooperação entre os Estados e a indústria privada no combate à cibercriminalidade, bem como a necessidade de proteger os interesses legítimos ligados ao uso e desenvolvimento das tecnologias de informação;

Acreditando que uma luta efectiva contra a cibercriminalidade requer uma cooperação internacional em matéria penal acrescida, rápida e eficaz;

A Convenção de Budapeste classifica os crimes de informática³¹.

Infracções penais contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos: acesso legítimo; interceptação ilegítima; interferência em dados; interferência em sistemas e uso indevido de dispositivos.

Infracções penais relacionadas com computadores: falsidade informática, burla informática.

Infracções penais relacionadas com o conteúdo: infracções penais relacionadas a pornografia infantil

Infracções penais relacionadas com a violação do direito do autor e direitos conexos.

Da maneira que determina a convenção, facilita bastante o combate e aplicação das devidas penas aos “delinquentes cibernéticos”.

8.2 Itália

²⁹ **Convenção sobre o Cibercrime.** Disponível em: pt.wikipedia.org/wiki/convenção_sobre_o_cibercrime. Acesso em 29 de outubro de 2013.

³⁰ Convenção de Budapeste. Disponível em: www.wirelessbrasil.org/wirwlessbr/secoes/crimes_digitais/texto_convencao.pdf. Acesso em 29 de outubro de 2013

³¹ Convenção de Budapeste. Disponível em: www.wirelessbrasil.org/wirwlessbr/secoes/crimes_digitais/texto_convencao.pdf. Acesso em 29 de outubro de 2013.

A Itália dispõe de uma legislação bastante completa no que tange o tema da informática. A Lei nº 547/93, vigente a mais de treze anos, segundo Carla Rodrigues³², “acrescentou quinze figuras típicas, sendo seis figuras essenciais: sabotagem, acesso ilegal, violação de segredo informático e do sigilo, falsificações, fraude informática e violação dos direitos do autor concernentes ao *software*. ”

No país, enviar vírus também tem tipificação própria, logo é de fato considerado crime. A conduta está prevista no art. 615, do Código Penal Italiano.

8.3 Inglaterra

A Inglaterra não fica para trás. Sua lei chefe de combate aos crimes informáticos é o *Computer Misuse Act*.

Sobre a referida lei, Fabrício Rosa³³ comenta:

A lei inglesa que dispõe a respeito dos “crimes de informática” foi elaborada em 1990, quando foi introduzido, no ordenamento jurídico, o delito de acesso não-autorizado, dispondo no art. 3º, inc. 2º, que a pessoa deve ter a intenção de modificar o conteúdo de qualquer computador através dos seguintes comportamentos:

- *impedindo a operação de computador; ou
- *impedindo ou dificultando o acesso a qualquer programa, ou a confiança desses dados;
- *impedindo a execução de qualquer dos programas, ou a confiança desses dados.

8.4 Estados Unidos

Um dos primeiros a se manifestar, em termos de legislação, acerca dos crimes virtuais. Já em 1970 os Estados Unidos legislava sobre o tópico, e em 1986 criou o *Computer Fraud and Abuse Act* – CFAA.

Carla Rodrigues (2003, p.161) elenca as principais leis:

Os Estados Unidos possuem várias leis sobre a informática. A Lei 18 U.S.C. 1362 protegendo as linhas de comunicação,

³²CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática: e seus Aspectos Processuais**. 2. Ed. Rio de Janeiro: Lúmem Júris, 2003, p.158.

³³ROSA, Fabrício. **Crimes de Informática**. 2.ed. Campinas: BookSeller, 2006.

estacoes e sistemas. A Lei 18 U.S.C. 2511 tutela as comunicações tipificando como crime a conduta de quem intercepta ou revela comunicação, oral ou eletrônica, proibida. A Lei 18 U.S.C. 2701 tipifica o acesso ilícito de comunicações armazenadas. E a lei 18 U.S.C. 2702 dispõe sobre a revelação de conteúdo. Além de outras mais.

Após o ataque às Torres Gêmeas, a cautela dos americanos aumentou, logo criaram novas leis: USAPA- USA *PatrioticAct*, FISA – *ForeignIntelligenceSurvaillancAct* e CSEA – *CybersecurityEnhancementAct*, todas visando combater o *cyberterrorismo*.

9.0 CONCLUSÃO

Da época em que o Código Penal Brasileiro foi idealizado (1940) até o presente momento, diversas mudanças ocorreram, e sempre ocorrem, em nossa sociedade. O exponencial avanço tecnológico, especificamente na área da informática, faz parte dessas mudanças. Entretanto, o Direito, que tem o dever de acompanhar as transformações sociais, não foi capaz de conduzi-la na mesma velocidade em que a chamada tecnologia da informação se propaga.

Com o desenvolvimento deste artigo, verificou-se que a ascensão do universo virtual propiciou uma nova dimensão à criminalidade, a qual o Brasil encontra-se despreparado para lidar. O país, ao contrário de diversas outras nações, carece de legislação específica para coordenar o assunto. Salvo algumas iniciativas de Projetos de Lei que objetivam a regulamentação dos delitos cibernéticos, e poucas leis já vigentes.

O Brasil ainda não se encontra preparado para combater efetivamente a execução de tais crimes, seja pela falta de investimento na área, pelo despreparo e carência dos órgãos especializados e principalmente pela lacuna legal existente. Somente a devida tipificação da conduta ilícita envolvendo sistemas computacionais tornará o agente passivo da punição adequada. Por isso, torna-se imprescindível a criação de uma legislação específica ou a adequação da existente com relação aos chamados crimes de informática.

REFERÊNCIAS

ARAS, Vladimir. **Crimes de Informática. Uma nova criminalidade**. Jus Navigandi, n.51. Disponível em: <http://jus2.uol.com.br/doutrina/texto.aspx?id=2250>>. Acesso em 28 de out. 2013.

BRASIL. “Lei Carolina Dieckmann” sobre crimes da internet entra em vigor. Disponível em <http://tecnologia.uol.com.br/noticias/redacao/2013/04/02/lei-carolina-dieckmann-sobre-crimes-na-internet-entra-em-vigor.htm>. Acesso em 8 de novembro de 2013.

BRASIL. Brito Auriney. Análise da lei 12.12737/12- “Lei Carolina Dieckmann”. Disponível em <http://atualidadesdodireito.com.br/aurineybrito/2013/04/03/analise-da-lei-12-73712-lei-carolina-dieckmann/>. Acesso em 9 de novembro de 2013.

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constitui%C3%A7ao.htm. Acesso em 3 de novembro de 2013.

BRASIL. Convenção de Budapeste. Disponível em: www.wirelessbrasil.org/wirwlessbr/secoes/crimes_digitais/texto_convencao.pdf. Acesso em 29 de outubro de 2013.

BRASIL. Convenção sobre o Cibercrime. Disponível em: pt.wikipedia.org/wiki/conven%C3%A7%C3%A3o_sobre_o_cibercrime. Acesso em 29 de outubro de 2013.

BRASIL. Decreto-Lei nº 2.848 de 7 de dezembro de 1940. Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compiladp.htm. Acesso em 28 de outubro de 2013.

CAPEZ, Fernando. **Curso de Direito Penal, volume 1: parte geral**. São Paulo. Saraiva, 2010.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. 2. Ed. Rio de Janeiro, Lumem Juris, 2003.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo. Saraiva, 2001.

FELICIANO, Guilherme Guimarães. **Informática e Criminalidade: Primeiras Linhas**. Ribeirão Preto: Nacional de Direito, 2001.

MIRABETE, Júlio Fabbrini. **Processo Penal**. 18. Rd. São Paulo: Atlas, 2008.

MIRANDA, Murilo. **Da Persecução Penal dos Crimes Virtuais**. Disponível em http://www.jurisway.org.br/monografias/monografia.asp?id_dh=9903. Acesso em 15 de outubro de 2013

NOGUEIRA, Sandro D`Amato. **Crimes de Informática**. São Paulo: BH Editora, 2009.

ROSA, Fabrício. **Crimes de Informática**. 2.ed. Campinas: BookSeller, 2006.

SILVA, Marco Antônio Marques de. **Acesso à Justiça Penal e Estado Democrático de Direito**. São Paulo, Ed. J. de Oliveira, 2001.